RoamAbout®

Mobility System Software

Command Line Interface Reference
Version 5.0

P/N 9034145-04

enterasys®

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

© 2006 Enterasys Networks, Inc. All rights reserved.

Part Number: 9034145-04 November 2006

ENTERASYS, ENTERASYS NETWORKS, ENTERASYS ROAMABOUT, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc. in the United States and other countries. All other product names mentioned in this manual may be trademarks or registered trademarks of their respective owners.

Documentation URL: http://www.enterasys.com/support/manuals

Documentacion URL: http://www.enterasys.com/support/manuals

Dokumentation im Internet: http://www.enterasys.com/support/manuals

Enterasys Networks, Inc.
Firmware License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between the end user ("You") and Enterasys Networks, Inc. on behalf of itself and its Affiliates (as hereinafter defined) ("Enterasys") that sets forth Your rights and obligations with respect to the Enterasys software program/firmware installed on the Enterasys product (including any accompanying documentation, hardware or media) ("Program") in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. "Affiliate" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, and supersedes all prior discussions, representations, understandings or agreements, whether oral or in writing, between the parties with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, "YOU" AND "YOUR" SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

You and Enterasys agree as follows:

1. **LICENSE.** You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.

2. **RESTRICTIONS.** Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:

   (i) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys' applicable fee.

   (ii) Incorporate the Program, in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.

   (iii) Publish, disclose, copy, reproduce or transmit the Program, in whole or in part.

   (iv) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.

   (v) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.

3. **APPLICABLE LAW.** This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on Contracts for the International Sale of Goods, the United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

4. **EXPORT RESTRICTIONS.** You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the Program is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. **DISCLAIMER OF WARRANTY.** EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY Enterasys, Enterasys DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON- INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

7. **LIMITATION OF LIABILITY.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. **AUDIT RIGHTS.** You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

9. **OWNERSHIP.** This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

10. **ENFORCEMENT.** You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

11. **ASSIGNMENT.** You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock or assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

12. **WAIVER.** A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

13. **SEVERABILITY.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

14. **TERMINATION.** Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

Enterasys Networks, Inc. Software License Agreement

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc. ("Enterasys") that sets forth your rights and obligations with respect to the software contained in CD-ROM or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, INC. (978) 684-1000. ATTN: LEGAL DEPARTMENT.

Enterasys will grant You a non-transferable, nonexclusive license to use the enclosed machine-readable form of software (the "Licensed Software") and the accompanying documentation (the Licensed Software, the media embodying the Licensed Software, and the documentation are collectively referred to in this Agreement as the "Licensed Materials") on one single computer if You agree to the following terms and conditions:

1. **TERM.** This Agreement is effective from the date on which You open the package containing the Licensed Materials. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and your license to use the Licensed Materials will also terminate if You fail to comply with any term or condition herein.

2. **GRANT OF SOFTWARE LICENSE.** The license granted to You by Enterasys when You open this sealed package authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

3. **RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS**. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Enterasys' prior written consent, and in no event shall You operate more than one copy of the Licensed Software. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement.

You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

4. **TITLE AND PROPRIETARY RIGHTS**.

   (a) The Licensed Materials are copyrighted works and are the sole and exclusive property of Enterasys, any company or a division thereof which Enterasys controls or is controlled by, or which may result from the merger or consolidation with Enterasys (its "affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

   (b) You further acknowledge that in the event of a breach of this Agreement, Enterasys shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Enterasys shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Enterasys.

5. **PROTECTION AND SECURITY**. You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Enterasys or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Enterasys. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Enterasys of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Enterasys or its Affiliates and/or its/their software suppliers.

6. **MAINTENANCE AND UPDATES**. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of a Enterasys Service and Maintenance Agreement, if Enterasys and You enter into such an agreement. Except as specifically set forth in such agreement, Enterasys shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

7. **DEFAULT AND TERMINATION**. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Enterasys, Enterasys may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Enterasys and You.

(a) Immediately after termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Enterasys the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Enterasys.

(b) Sections 4, 5, 7, 8, 9, 10, 11, and 12 shall survive termination of this Agreement for any reason.

8. **EXPORT REQUIREMENTS**. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Licensed Materials are exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Licensed Materials and agree that You will use the Licensed Materials for civil end uses only and not for military purposes.

If the Licensed Materials are exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Section 4 of this Agreement, You agree not to (i) reexport or release the Licensed Software, the source code for the Licensed Software or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Licensed Software or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant o r any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

9. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS**. The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

10. **LIMITED WARRANTY AND LIMITATION OF LIABILITY**. The only warranty Enterasys makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Enterasys in good faith determines that the media and proof of payment of the license fee are returned to Enterasys or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.

NEITHER ENTERASYS NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL ENTERASYS OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF ENTERASYS OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ENTERASYS OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

11. **JURISDICTION**. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the Commonwealth of Massachusetts, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts.

12. **GENERAL**.

(a) This Agreement shall not be assignable by You without the express written consent of Enterasys. The rights of Enterasys and Your obligations under this Agreement shall inure to the benefit of Enterasys' assignees, licensors, and licensees.

(b) Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

(c) The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

(d) Enterasys' waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

(e) Should You have any questions regarding this Agreement, You may contact Enterasys at the address set forth below. Any notice or other communication to be sent to Enterasys must be mailed by certified mail to the following address: ENTERASYS NETWORKS, INC., 50 Minuteman Road, Andover, MA 01810 Attn: Manager - Legal Department.

Contents

About This Guide

Introducing Mobility System Software xxi
Documentation xxii
Planning, Configuration, and Deployment xxii
Installation xxii
Configuration and Management xxii
Safety and Advisory Notices xxii
Text and Syntax Conventions xxiii
Getting Help xxiii

Chapter 1: Using the Command-Line Interface

CLI Conventions 1-1
Command Prompts 1-2
Syntax Notation 1-2
Text Entry Conventions and Allowed Characters 1-2
MAC Address Notation 1-3
IP Address and Mask Notation 1-3
Subnet Masks 1-3
Wildcard Masks 1-3
User Globs, MAC Address Globs, and VLAN Globs 1-3
User Globs 1-3
MAC Address Globs 1-4
VLAN Globs 1-4
Matching Order for Globs 1-5
Port Lists 1-5
Virtual LAN Identification 1-5
Command-Line Editing 1-6
Keyboard Shortcuts 1-6
History Buffer 1-6
Tabs 1-6
Single-Asterisk (*) Wildcard Character 1-7
Double-Asterisk (**) Wildcard Characters 1-7
Using CLI Help 1-7
Understanding Command Descriptions 1-8

Chapter 2: Access Commands

disable 2-2
enable 2-3
quit 2-4
set enablepass 2-5

Chapter 3: System Services Commands

clear banner motd 3-2
clear history 3-3
clear prompt 3-4
clear system 3-5
help 3-6

history 3-7
set auto-config 3-8
set banner motd 3-10
set confirm 3-11
set length 3-12
set license 3-13
set prompt 3-14
set system contact 3-15
set system countrycode 3-16
set system idle-timeout 3-19
set system ip-address 3-20
set system location 3-21
set system name 3-22
show banner motd 3-23
show load 3-24
show licenses 3-25
show system 3-26
show tech-support 3-28

Chapter 4: Port Commands

clear dap 4-2
clear port counters 4-3
clear port-group 4-4
clear port media-type 4-5
clear port mirror 4-6
clear port name 4-7
clear port type 4-8
monitor port counters 4-10
reset port 4-14
set dap 4-15
set port 4-17
set port-group 4-18
set port media-type 4-19
set port mirror 4-20
set port name 4-21
set port negotiation 4-22
set port speed 4-24
set port trap 4-25
set port type wired-auth 4-26
show port counters 4-28
show port-group 4-29
show port media-type 4-30
show port status 4-31

Chapter 5: VLAN Commands

clear fdb 5-2
clear security l2-restrict 5-4
clear security l2-restrict counters 5-5
clear vlan 5-6
set fdb 5-8
set fdb agingtime 5-9
set security l2-restrict 5-10
set vlan name 5-11

set vlan port 5-12
set vlan tunnel-affinity 5-13
show fdb 5-14
show fdb agingtime 5-16
show fdb count 5-17
show roaming station 5-18
show roaming vlan 5-20
show security l2-restrict 5-21
show tunnel 5-23
show vlan config 5-24

Chapter 6: QoS Commands

clear qos 6-2
set qos cos-to-dscp-map 6-3
set qos dscp-to-cos-map 6-4
show qos 6-5
show qos dscp-table 6-6

Chapter 7: IP Services Commands

clear interface 7-4
clear ip alias 7-5
clear ip dns domain 7-6
clear ip dns server 7-7
clear ip route 7-8
clear ip telnet 7-9
clear ntp server 7-10
clear ntp update-interval 7-11
clear snmp community 7-12
clear snmp notify target 7-13
clear snmp notify profile 7-14
clear snmp trap receiver 7-15
clear snmp usm 7-16
clear summertime 7-17
clear system ip-address 7-18
clear timezone 7-19
ping 7-20
set arp 7-22
set arp agingtime 7-23
set interface 7-24
set interface dhcp-client 7-25
set interface dhcp-server 7-26
set interface status 7-28
set ip alias 7-29
set ip dns 7-30
set ip dns domain 7-31
set ip dns server 7-32
set ip https server 7-33
set ip route 7-34
set ip snmp server 7-36
set ip ssh 7-37
set ip ssh server 7-38
set ip telnet 7-39
set ip telnet server 7-40

set ntp 7-41
set ntp server 7-42
set ntp update-interval 7-43
set snmp community 7-44
set snmp notify target 7-46
SNMPv3 with Traps 7-47
SNMPv2c with Informs 7-48
SNMPv2c with Traps 7-48
SNMPv1 with Traps 7-49
set snmp profile 7-51
set snmp protocol 7-56
set snmp security 7-57
set snmp trap 7-58
set snmp trap receiver 7-59
set snmp usm 7-60
set summertime 7-63
set system ip-address 7-65
set timedate 7-66
set timezone 7-67
show arp 7-68
show dhcp-client 7-70
show dhcp-server 7-72
show interface 7-75
show ip alias 7-77
show ip dns 7-78
show ip https 7-80
show ip route 7-82
show ip telnet 7-84
show ntp 7-85
show snmp configuration 7-87
show snmp community 7-89
show snmp counters 7-90
show snmp notify profile 7-91
show snmp notify target 7-92
show snmp status 7-93
show snmp usm 7-94
show summertime 7-95
show timedate 7-96
show timezone 7-97
telnet 7-98
traceroute 7-100

Chapter 8: AAA Commands

clear accounting 8-3
clear authentication admin 8-4
clear authentication console 8-5
clear authentication dot1x 8-6
clear authentication mac 8-7
clear authentication proxy 8-8
clear authentication web 8-9
clear location policy 8-10
clear mac-user 8-11
clear mac-user attr 8-12

clear mac-user group 8-13
clear mac-usergroup 8-14
clear mac-usergroup attr 8-15
clear mobility-profile 8-16
clear user 8-17
clear user attr 8-18
clear user group 8-19
clear usergroup 8-20
clear usergroup attr 8-21
set accounting {admin | console} 8-22
set accounting {dot1x | mac | web | last-resort} 8-24
set accounting system 8-26
set authentication admin 8-27
set authentication console 8-29
set authentication dot1x 8-31
set authentication mac 8-35
set authentication proxy 8-37
set authentication web 8-38
set location policy 8-40
set mac-user 8-43
set mac-user attr 8-44
set mac-usergroup attr 8-50
set mobility-profile 8-52
set mobility-profile mode 8-54
set user 8-55
set user attr 8-57
set user group 8-58
set usergroup 8-59
set web-portal 8-61
show aaa 8-62
show accounting statistics 8-65
show location policy 8-68
show mobility-profile 8-69

Chapter 9: Mobility Domain Commands

clear domain security 9-2
clear mobility-domain 9-3
clear mobility-domain member 9-4
set domain security 9-5
set mobility-domain member 9-6
set mobility-domain mode member seed-ip 9-7
set mobility-domain mode seed domain-name 9-8
show mobility-domain config 9-9
show mobility-domain 9-10

Chapter 10: Network Domain Commands

clear network-domain 10-2
clear network-domain mode 10-3
clear network-domain peer 10-4
clear network-domain seed-ip 10-5
set network-domain mode member seed-ip 10-6
set network-domain peer 10-7

set network-domain mode seed domain-name 10-8
show network-domain 10-9

Chapter 11: Access Point Commands

clear {ap | dap} radio 11-5
clear dap boot-configuration 11-7
clear radio-profile 11-8
clear service-profile 11-10
reset {ap | dap} 11-12
set dap auto 11-13
set dap auto mode 11-15
set dap auto persistent 11-16
set dap auto radiotype 11-17
set {ap | dap} bias 11-18
set {ap | dap} blink 11-19
set dap boot-ip 11-20
set dap boot-switch 11-22
set dap boot-vlan 11-24
set {ap | dap} contact 11-25
set dap fingerprint 11-26
set {ap | dap} force-image-download 11-27
set {ap | dap} group 11-28
set {ap | dap} image 11-29
set {ap | dap} location 11-29
set {ap | dap} name 11-30
set {ap | dap} radio antenna-location 11-31
set {ap | dap} radio antennatype 11-32
set {ap | dap} radio auto-tune max-power 11-33
set {ap | dap} radio auto-tune max-retransmissions 11-34
set {ap | dap} radio auto-tune min-client-rate 11-34
set {ap | dap} radio channel 11-35
set {ap | dap} radio auto-tune min-client-rate 11-36
set {ap | dap} radio mode 11-38
set {ap | dap} radio radio-profile 11-39
set {ap | dap} radio tx-power 11-40
set dap security 11-42
set {ap | dap} upgrade-firmware 11-44
set radio-profile active-scan 11-45
set radio-profile auto-tune channel-config 11-46
set radio-profile auto-tune channel-holddown 11-48
set radio-profile auto-tune channel-interval 11-49
set radio-profile auto-tune channel-lockdown 11-50
set radio-profile auto-tune power-backoff-timer 11-51
set radio-profile auto-tune power-config 11-52
set radio-profile auto-tune power-interval 11-53
set radio-profile auto-tune power-lockdown 11-54
set radio-profile auto-tune power-ramp-interval 11-55
set radio-profile beacon-interval 11-56
set radio-profile countermeasures 11-57
set radio-profile dtim-interval 11-58
set radio-profile frag-threshold 11-59
set radio-profile max-rx-lifetime 11-61
set radio-profile max-tx-lifetime 11-62

set radio-profile mode 11-63
set radio-profile preamble-length 11-66
set radio-profile qos-mode 11-67
set radio-profile rfid-mode 11-68
set radio-profile rts-threshold 11-69
set radio-profile service-profile 11-70
set radio-profile wmm 11-76
set radio-profile wmm-powersave 11-77
set service-profile attr 11-78
set service-profile auth-dot1x 11-80
set service-profile auth-fallthru 11-82
set service-profile auth-psk 11-84
set service-profile beacon 11-85
set service-profile cac-mode 11-86
set service-profile cac-session 11-87
set service-profile cipher-ccmp 11-88
set service-profile cipher-tkip 11-89
set service-profile cipher-wep104 11-90
set service-profile cipher-wep40 11-91
set service-profile cos 11-92
set service-profile dhcp-restrict 11-93
set service-profile idle-client-probing 11-94
set service-profile keep-initial-vlan 11-95
set service-profile long-retry-count 11-96
set service-profile no-broadcast 11-97
set service-profile proxy-arp 11-99
set service-profile psk-phrase 11-100
set service-profile psk-raw 11-101
set service-profile rsn-ie 11-102
set service-profile shared-key-auth 11-103
set service-profile short-retry-count 11-104
set service-profile soda agent-directory 11-105
set service-profile soda enforce-checks 11-106
set service-profile soda failure-page 11-108
set service-profile soda logout-page 11-109
set service-profile soda mode 11-110
set service-profile soda remediation-acl 11-111
set service-profile soda success-page 11-112
set service-profile ssid-name 11-113
set service-profile ssid-type 11-114
set service-profile static-cos 11-115
set service-profile tkip-mc-time 11-116
set service-profile transmit-rates 11-117
set service-profile user-idle-timeout 11-119
set service-profile web-portal-acl 11-120
set service-profile web-portal-form 11-121
set service-profile web-portal-session-timeout 11-123
set service-profile wep active-multicast-index 11-124
set service-profile wep active-unicast-index 11-125
set service-profile wep key-index 11-126
set service-profile wpa-ie 11-127
show {ap | dap} config 11-128
show {ap | dap} counters 11-132
show {ap | dap} qos-stats 11-135

show {ap | dap} etherstats 11-137
show {ap | dap} group 11-139
show {ap | dap} status 11-140
show auto-tune attributes 11-145
show auto-tune neighbors 11-147
show dap boot-configuration 11-149
show dap connection 11-151
show dap global 11-153
show dap unconfigured 11-155
show radio-profile 11-157
show service-profile 11-160

Chapter 12: STP Commands

clear spantree portcost 12-2
clear spantree portpri 12-3
clear spantree portvlancost 12-4
clear spantree portvlanpri 12-5
clear spantree statistics 12-6
set spantree 12-7
set spantree backbonefast 12-8
set spantree fwddelay 12-9
set spantree hello 12-10
set spantree maxage 12-11
set spantree portcost 12-12
set spantree portfast 12-14
set spantree portpri 12-15
set spantree portvlancost 12-16
set spantree portvlanpri 12-17
set spantree priority 12-18
set spantree uplinkfast 12-19
show spantree 12-20
show spantree backbonefast 12-23
show spantree blockedports 12-24
show spantree portfast 12-25
show spantree portvlancost 12-27
show spantree statistics 12-28
show spantree uplinkfast 12-33

Chapter 13: IGMP Snooping Commands

clear igmp statistics 13-2
set igmp 13-3
set igmp lmqi 13-4
set igmp mrouter 13-5
set igmp mrsol 13-6
set igmp mrsol mrsi 13-7
set igmp oqi 13-8
set igmp proxy-report 13-9
set igmp qi 13-10
set igmp qri 13-11
set igmp querier 13-12
set igmp receiver 13-13
set igmp rv 13-14
show igmp 13-15

show igmp mrouter 13-19
show igmp querier 13-21
show igmp receiver-table 13-23
show igmp statistics 13-25

Chapter 14: Security ACL Commands

clear security acl 14-2
clear security acl map 14-4
commit security acl 14-6
rollback security acl 14-8
set security acl 14-9
set security acl map 14-14
set security acl hit-sample-rate 14-16
show security acl 14-17
show security acl editbuffer 14-18
show security acl hits 14-19
show security acl info 14-20
show security acl map 14-22
show security acl resource-usage 14-23

Chapter 15: Cryptography Commands

crypto ca-certificate 15-2
crypto certificate 15-4
crypto generate key 15-6
crypto generate request 15-7
crypto generate self-signedweb 15-9
crypto otp 15-11
crypto pkcs12 15-13
show crypto ca-certificate 15-15
show crypto certificate 15-17
show crypto key domain 15-18
show crypto key ssh 15-19

Chapter 16: RADIUS and Server Groups Commands

clear radius 16-2
clear radius client system-ip 16-4
clear radius proxy client 16-5
clear radius proxy port 16-6
clear radius server 16-7
clear server group 16-8
set radius 16-9
set radius client system-ip 16-11
set radius proxy client 16-12
set radius proxy port 16-13
set radius server 16-14
set server group 16-16
set server group load-balance 16-17

Chapter 17: 802.1X Management Commands

clear dot1x bonded-period 17-3
clear dot1x max-req 17-4
clear dot1x port-control 17-5

clear dot1x quiet-period 17-6
clear dot1x reauth-max 17-7
clear dot1x reauth-period 17-8
clear dot1x timeout auth-server 17-9
clear dot1x timeout supplicant 17-10
clear dot1x tx-period 17-11
set dot1x authcontrol 17-12
set dot1x bonded-period 17-13
set dot1x key-tx 17-14
set dot1x max-req 17-15
set dot1x port-control 17-16
set dot1x quiet-period 17-17
set dot1x reauth 17-18
set dot1x reauth-max 17-19
set dot1x reauth-period 17-20
set dot1x timeout auth-server 17-21
set dot1x timeout supplicant 17-22
set dot1x tx-period 17-23
set dot1x wep-rekey 17-24
set dot1x wep-rekey-period 17-25
show dot1x 17-26

Chapter 18: Session Management Commands

clear sessions 18-2
clear sessions network 18-3
show sessions 18-5
show sessions network 18-7

Chapter 19: RF Detection Commands

clear rfdetect attack-list 19-3
clear rfdetect black-list 19-4
clear rfdetect countermeasures mac 19-5
clear rfdetect ignore 19-6
clear rfdetect ssid-list 19-7
clear rfdetect vendor-list 19-8
set rfdetect attack-list 19-9
set rfdetect black-list 19-10
set rfdetect ignore 19-11
set rfdetect log 19-12
set rfdetect signature 19-13
set rfdetect ssid-list 19-14
set rfdetect vendor-list 19-15
show rfdetect attack-list 19-16
show rfdetect black-list 19-17
show rfdetect clients 19-18
show rfdetect countermeasures 19-21
show rfdetect data 19-23
show rfdetect ignore 19-25
show rfdetect mobility-domain 19-26
show rfdetect ssid-list 19-30
show rfdetect vendor-list 19-31

show rfdetect visible 19-32
test rflink 19-35

Chapter 20: File Management Commands

backup 20-2
clear boot config 20-4
copy 20-5
delete 20-7
dir 20-8
install soda agent 20-10
load config 20-11
md5 20-13
mkdir 20-14
reset system 20-16
restore 20-17
rmdir 20-19
save config 20-20
set boot configuration-file 20-21
set boot image 20-22
set boot partition 20-23
show boot 20-24
show config 20-26
show version 20-28
uninstall soda agent 20-30

Chapter 21: Trace Commands

clear log trace 21-2
clear trace 21-3
save trace 21-4
set trace authentication 21-5
set trace authorization 21-6
set trace dot1x 21-7
set trace sm 21-8
show trace 21-9

Chapter 22: Snoop Commands

clear snoop 22-2
clear snoop map 22-3
set snoop 22-4
set snoop map 22-6
set snoop mode 22-7
show snoop 22-8
show snoop info 22-9
show snoop map 22-10
show snoop stats 22-11

Chapter 23: System Log Commands

clear log 23-2
set log 23-3
set log mark 23-6
show log buffer 23-7

show log config 23-9
show log trace 23-10

Chapter 24: Boot Prompt Commands

autoboot 24-2
boot 24-3
change 24-5
create 24-6
delete 24-7
dhcp 24-8
diag 24-9
dir 24-10
fver 24-11
help 24-12
ls 24-13
next 24-14
reset 24-15
show 24-16
test 24-18
version 24-19

Index

Command Index

About This Guide

For information about...	Refer to page...
Introducing Mobility System Software	xxi
Documentation	xxii
Getting Help	xxiii

This command reference explains Mobility System Software (MSS) command line interface (CLI) commands that you enter on a RoamAbout Switch (called RoamAbout Switch, RBT switch, or RAS in this document) to configure and manage the Mobility System wireless LAN (WLAN).

Read this reference if you are a network administrator responsible for managing RoamAbout Switches and RoamAbout Access Points (APs) in a network.

Introducing Mobility System Software

The Mobility System is an enterprise-class WLAN solution that seamlessly integrates with an existing wired enterprise network. The Mobility System provides secure connectivity to both wireless and wired users in large environments such as office buildings, hospitals, and university campuses and in small environments such as branch offices.

The Mobility System fulfills the three fundamental requirements of an enterprise WLAN: It eliminates the distinction between wired and wireless networks, allows users to work safely from anywhere (*secure mobility*), and provides a comprehensive suite of intuitive tools for planning and managing the network before and after deployment, greatly easing the operational burden on IT resources.

The Mobility System consists of the following components:

- **RoamAbout Switch Manager (RASM) tool suite**—A full-featured graphical user interface (GUI) application used to plan, configure, deploy, and manage a WLAN and its users
- **One or more RoamAbout Switches** —Distributed, intelligent machines for managing user connectivity, connecting and powering access points, and connecting the WLAN to the wired network backbone
- **Multiple Access Points (APs)**—Wireless access points that transmit and receive radio frequency (RF) signals to and from wireless users and connect them to a RoamAbout Switch
- **Mobility System Software (MSS)**—The operating system that runs all RoamAbout Switches and access points in a WLAN, and is accessible through a command-line interface (CLI), the WebView interface, or the RoamAbout Switch Manager GUI

Documentation

Consult the following documents to plan, install, configure, and manage a Mobility System.

Planning, Configuration, and Deployment

RoamAbout Switch Manager User's Guide. Instructions for planning, configuring, deploying, and managing the entire WLAN with the RoamAbout Switch Manager (RASM) tool suite. Read this guide to learn how to plan wireless services, how to configure and deploy RoamAbout equipment to provide those services, and how to optimize and manage your WLAN.

RoamAbout Switch Manager Interface Reference. Detailed instructions and information for all RoamAbout Switch Manager planning, configuration, and management features.

Installation

- *RoamAbout Wireless Switch Installation Guide*. Instructions and specifications for installing the RBT-8100, RBT-8200, and the RBT-8400, in a Mobility System WLAN, connecting it to a RoamAbout Switch and instructions for performing basic setup of secure (802.1X) and guest (WebAAA™) access, for configuring a Mobility Domain for roaming, and basic instructions for deploying a secure IEEE 802.11 wireless service
- *Enterasys Regulatory Information*. Important safety instructions and compliance information that you must read before installing Enterasys Networks products

Configuration and Management

- *RoamAbout Switch Manager Interface Reference*. Instructions for planning, configuring, deploying, and managing the entire WLAN with the RoamAbout Switch Manager tool suite
- *RoamAbout Mobility System Software Configuration Guide*. Instructions for configuring and managing the system through the MSS CLI
- *RoamAbout Mobility System Software Command Line Interface Reference*. Functional reference to all MSS commands supported on RoamAbout Switches and access points

Safety and Advisory Notices

The following kinds of safety and advisory notices appear in this manual.

Note: This information is of special interest.

Caution: Contains information essential to avoid damage to the equipment.

Text and Syntax Conventions

RoamAbout Switch manuals use the following text and syntax conventions:

Convention	Use
`Monospace text`	Sets off command syntax or sample commands and system responses.
Blue text	Indicates a hyperlink
Bold text	Highlights commands that you enter or items you select.
Italic text	Designates command variables that you replace with appropriate values, or highlights publication titles or words requiring special emphasis.
Menu Name > **Command**	Indicates a menu item that you select. For example, **File** > **New** indicates that you select **New** from the File menu.
[ ] (square brackets)	Enclose optional parameters in command syntax.
{ } (curly brackets)	Enclose mandatory parameters in command syntax.
| (vertical bar)	Separates mutually exclusive options in command syntax.

Getting Help

For additional support related to the product or this document, contact Enterasys Networks using one of the following methods:

World Wide Web	http://www.enterasys.com/services/support/
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 For the Enterasys Networks Support toll-free number in your country: http://www.enterasys.com/services/support/contact/
Internet mail	**support@enterasys.com** To expedite your message, please type **[RoamAbout]** in the subject line.
To send comments concerning this document to the Technical Publications Department: **techpubs@enterasys.com** To expedite your message, please include the document Part Number in the email message.	

Before contacting Enterasys Networks for technical support, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network

- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

1

Using the Command-Line Interface

For information about...	Refer to page...
CLI Conventions	1-1
Command-Line Editing	1-6
Using CLI Help	1-7
Understanding Command Descriptions	1-8

Mobility System Software (MSS) operates a Mobility System wireless LAN (WLAN) consisting of RoamAbout Switch Manager (RASM) software, RoamAbout Switches (called RoamAbout Switch or RAS in this document), and RoamAbout access points. MSS has a command-line interface (CLI) on the RAS that you can use to configure and manage the switch and its attached access points.

You configure the RAS and access points primarily with **set**, **clear**, and **show** commands. Use **set** commands to change parameters. Use **clear** commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another **set** command. Use **show** commands to display the current configuration and monitor the status of network operations.

The RAS supports two connection modes:

- Administrative access mode, which enables the network administrator to connect *to* the RAS and configure the network
- Network access mode, which enables network users to connect *through* the RAS to access the network

CLI Conventions

Be aware of the following MSS CLI conventions for command entry:

- Command Prompts on page 1-2
- Syntax Notation on page 1-2
- Text Entry Conventions and Allowed Characters on page 1-2
- User Globs, MAC Address Globs, and VLAN Globs on page 1-3
- Port Lists on page 1-5
- Virtual LAN Identification on page 1-5

Command Prompts

By default, the MSS CLI provides the following prompt for restricted users. The *mm* portion shows the RAS model number (for example, *20*) and the *nnnnnn* portion shows the last 6 digits of the switch's media access control (MAC) address.

```
RBT-mm-nnnnnn>
```

After you become enabled as an administrative user by typing **enable** and supplying a suitable password, MSS displays the following prompt:

```
RBT-mm-nnnnnn#
```

For ease of presentation, this manual shows the restricted and enabled prompts as follows:

```
RBT-8100>
RBT-8100#
```

For information about changing the CLI prompt on a RAS, see set prompt on page 3-14.

Syntax Notation

The MSS CLI uses standard syntax notation:

- Bold monospace font identifies the command and keywords you must type. For example:

  set enablepass

- Italic monospace font indicates a placeholder for a value. For example, you replace *vlan-id* in the following command with a virtual LAN (VLAN) ID:

  clear interface *vlan-id* **ip**

- Curly brackets ({ }) indicate a mandatory parameter, and square brackets ([ ]) indicate an optional parameter. For example, you must enter **dynamic** or **port** and a port list in the following command, but a VLAN ID is optional:

  clear fdb {**dynamic** | **port** *port-list*} [**vlan** *vlan-id*]

- A vertical bar (|) separates mutually exclusive options within a list of possibilities. For example, you enter either **enable** or **disable**, not both, in the following command:

  set port {**enable** | **disable**} *port-list*

Text Entry Conventions and Allowed Characters

Unless otherwise indicated, the MSS CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

Enterasys Networks recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACLs). For example, do not configure two separate VLANs with the names *red* and *RED*.

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks (“”).

In addition, the CLI does not support the use of international characters such as the accented *É* in DÉCOR.

MAC Address Notation

MSS displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes—for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (-) or colon (:) delimiters, but colons are preferred.

For shortcuts:

- You can exclude leading zeros when typing a MAC address. MSS displays of MAC addresses include all leading zeros.
- In some specified commands, you can use the single-asterisk (*) wildcard character to represent from 1 byte to 5 bytes of a MAC address. (For more information, see MAC Address Globs on page 1-4.)

IP Address and Mask Notation

MSS displays IP addresses in dotted decimal notation—for example, 192.168.1.111. MSS makes use of both subnet masks and wildcard masks.

Subnet Masks

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks—for example, 192.168.1.112/24. You indicate the subnet mask with a forward slash (/) and specify the number of bits in the mask.

Wildcard Masks

Security access control lists (ACLs) use source and destination IP addresses and wildcard masks to determine whether the RAS filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any *0*s (zeros) in the mask, but does not check the bits that correspond to *1*s (ones) in the mask. You specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

The ACL mask must be a contiguous set of zeroes starting from the first bit. For example, 0.255.255.255, 0.0.255.255, and 0.0.0.255 are valid ACL masks. However, 0.255.0.255 is not a valid ACL mask.

User Globs, MAC Address Globs, and VLAN Globs

Name "globbing" is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. MSS accepts user globs, MAC address globs, and VLAN globs. The order in which globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs.

User Globs

A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user glob can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (**) wildcard characters with no delimiter characters match *all* usernames. The single-asterisk (*)

wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the *at* (@) sign and the period (.).

For example, the following globs identify the following users:

User Glob	User(s) Designated
jose@example.com	User *jose* at example.com
*@example.com	All users at example.com whose usernames do not contain periods—for example, jose@example.com and tamara@example.com, but *not* nin.wong@example.com, because nin.wong contains a period
*@marketing.example.com	All marketing users at example.com whose usernames do not contain periods
.@marketing.example.com	All marketing users at example.com whose usernames contain periods
*	All users with usernames that have no delimiters
EXAMPLE*	All users in the Windows Domain EXAMPLE with usernames that have no delimiters
EXAMPLE*.*	All users in the Windows Domain EXAMPLE whose usernames contain periods
**	All users

MAC Address Globs

A media access control (MAC) address glob is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address glob, you can use a single asterisk (*) as a wildcard to match *all* MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

```
00:*
00:01:*
00:01:02:*
00:01:02:03:*
00:01:02:03:04:*
```

For example, the MAC address glob 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identity (OUI).

VLAN Globs

A VLAN glob is a method for matching one of a set of local rules on a RAS, known as the location policy, to one or more users. MSS compares the VLAN glob, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine whether to apply the rule.

To match all VLANs, use the double-asterisk (**) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the glob, use the single-asterisk (*) wildcard. Valid VLAN glob delimiter characters are the *at* (@) sign and the period (.).

For example, the VLAN glob *bldg4.** matches *bldg4.security* and *bldg4.hr* and all other VLAN names with *bldg4.* at the beginning.

Matching Order for Globs

In general, the order in which you enter AAA commands determines the order in which MSS matches the user, MAC address, or VLAN to a glob. To verify the order, view the output of the **show aaa** or **show config** command. MSS checks globs that appear higher in the list before items lower in the list and uses the first successful match.

Port Lists

The physical Ethernet ports on a RAS can be set for connection to access points, authenticated wired users, or the network backbone. You can include a single port or multiple ports in one MSS CLI command by using the appropriate list format.

The ports on a RAS are numbered 1 through 2 or 4 depending on the switch. No port 0 exists on the switch. You can include a single port or multiple ports in a command that includes **port** *port-list*. Use one of the following formats for *port-list*:

- A single port number. For example:

  ```
  RBT-8100# set port enable 16
  ```

- A comma-separated list of port numbers, with no spaces. For example:

  ```
  RBT-8100# show port poe 1,2,4,13
  ```

- A hyphen-separated range of port numbers, with no spaces. For example:

  ```
  RBT-8100# reset port 12-16
  ```

- Any combination of single numbers, lists, and ranges. Hyphens take precedence over commas. For example:

  ```
  RBT-8100# show port status 1-3,14
  ```

Virtual LAN Identification

The *names* of virtual LANs (VLANs), which are used in Mobility Domain communications, are set by you and can be changed. In contrast, VLAN ID *numbers*, which the RAS uses locally, are determined when the VLAN is first configured and cannot be changed. Unless otherwise indicated, you can refer to a VLAN by either its VLAN name or its VLAN number. CLI **set** and **show** commands use a VLAN's name or number to uniquely identify the VLAN within the RAS.

Command-Line Editing

MSS editing functions are similar to those of many other network operating systems.

Keyboard Shortcuts

The following table lists the keyboard shortcuts for entering and editing CLI commands:

Keyboard Shortcut(s)	Function
Ctrl+A	Jumps to the first character of the command line.
Ctrl+B or Left Arrow key	Moves the cursor back one character.
Ctrl+C	Escapes and terminates prompts and tasks.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Jumps to the end of the current command line.
Ctrl+F or Right Arrow key	Moves the cursor forward one character.
Ctrl+K	Deletes from the cursor to the end of the command line.
Ctrl+L or Ctrl+R	Repeats the current command line on a new line.
Ctrl+N or Down Arrow key	Enters the next command line in the history buffer.
Ctrl+P or Up Arrow key	Enters the previous command line in the history buffer.
Ctrl+U or Ctrl+X	Deletes characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word typed.
Esc B	Moves the cursor back one word.
Esc D	Deletes characters from the cursor forward to the end of the word.
Delete key or Backspace key	Erases mistake made during command entry. Reenter the command after using this key.

History Buffer

The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

Tabs

The MSS CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to display the command(s) that begin with those characters. For example:

```
RBT-8100# show i <Tab>
ifm         Show interfaces maintained by the interface manager
igmp        Show igmp information
interface   Show interfaces
ip          Show ip information
```

Single-Asterisk (*) Wildcard Character

You can use the single-asterisk (*) wildcard character in globbing. (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 1-3.)

Double-Asterisk (**) Wildcard Characters

The double-asterisk (**) wildcard character matches all usernames. For details, see "User Globs" on page 1-3.

Using CLI Help

The CLI provides online help. To see the full range of commands available at your access level, type the **help** command. For example:

```
RBT-8100# help
Commands:
--------------------------------------------------------------------------
clear                Clear, use 'clear help' for more information
commit               Commit the content of the ACL table
copy                 Copy from filename (or url) to filename (or url)
crypto               Crypto, use 'crypto help' for more information
delete               Delete url
dir                  Show list of files on flash device
disable              Disable privileged mode
exit                 Exit from the Admin session
help                 Show this help screen
history              Show contents of history substitution buffer
load                 Load, use 'load help' for more information
logout               Exit from the Admin session
monitor              Monitor, use 'monitor help' for more information
ping                 Send echo packets to hosts
quit                 Exit from the Admin session
reset                Reset, use 'reset help' for more information
rollback             Remove changes to the edited ACL table
save                 Save the running configuration to persistent storage
set                  Set, use 'set help' for more information
show                 Show, use 'show help' for more information
telnet               telnet IP address [server port]
traceroute           Print the route packets take to network host
For more information on help, see "help" on page 3-6.
```

To see a subset of the online help, type the command for which you want more information. For example, to display all the commands that begin with the letter *i*, type the following command:

```
RBT-8100# show i?
ifm                  Show interfaces maintained by the interface manager
igmp                 Show igmp information
interface            Show interfaces
ip                   Show ip information
```

To see all the variations, type one of the commands followed by a question mark (?). For example:

```
RBT-8100# show ip ?
alias                Show ip aliases
dns                  show DNS status
https                show ip https
route                Show ip route table
telnet               show ip telnet
```

To determine the port on which Telnet is running, type the following command:

```
RBT-8100# show ip telnet
Server Status                Port
---------------------------------
Enabled                       23
```

Understanding Command Descriptions

Each command description in the Mobility System Software *Command Reference* contains the following elements:

- A command name, which shows the keywords but not the variables. For example, the following command name appears at the top of a command description and in the index:

  set {ap | dap} name

  The **set {ap | dap} name** command has the following complete syntax:

  set {**ap** *port-list* | **dap** *dap-num*} **name** *name*

- A brief description of the command's functions.
- The full command syntax.
- Any command defaults.
- The command access, which is either *enabled* or *all*. *All* indicates that anyone can access this command. *Enabled* indicates that you must enter the enable password before entering the command.
- The command history, which identifies the MSS version in which the command was introduced and the version numbers of any subsequent updates.
- Special tips for command usage. These are omitted if the command requires no special usage.
- One or more examples of the command in context, with the appropriate system prompt and response.
- One or more related commands.

2

Access Commands

Use access commands to control access to the Mobility System Software (MSS) (CLI). This chapter presents access commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
disable	2-2
enable	2-3
quit	2-4
set enablepass	2-5

disable

Changes the CLI session from enabled mode to restricted access.

Syntax

disable

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following command restricts access to the CLI for the current session:

```
RBT-8100# disable
RBT-8100>
```

Related Commands

enable on page 2-3

enable

Places the CLI session in enabled mode, which provides access to all commands required for configuring and monitoring the system.

Syntax

enable

Parameters

None.

Defaults

None.

Mode

All.

Usage

MSS displays a password prompt to challenge you with the enable password. To enable a session, your or another administrator must have configured the enable password to this RoamAbout switch with the **set enablepass** command.

Example

The following command plus the enable password provides enabled access to the CLI for the current sessions:

```
RBT-8100> enable
Enter password: password
RBT-8100#
```

Related Commands

- set enablepass on page 2-5
- set confirm on page 3-11

quit

Exit from the CLI session.

Syntax

quit

Parameters

None.

Defaults

None.

Mode

All.

Example

To end the administrator's session, type the following command:

```
RBT-8100> quit
```

set enablepass

Sets the password that provides enabled access (for configuration and monitoring) to the RoamAbout switch.

Note: The enable password is case-sensitive.

Syntax

```
set enablepass
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Usage

After typing the **set enablepass** command, press Enter. If you are entering the first enable password on this RoamAbout switch, press Enter at the *Enter old password* prompt. Otherwise, type the old password. Then type a password of up to 32 alphanumeric characters with no spaces, and reenter it at the *Retype new password* prompt.

Caution: Be sure to use a password that you will remember. If you lose the enable password, the only way to restore it causes the system to return to its default settings and wipes out the configuration.

Example

The following example illustrates the prompts that the system displays when the enable password is changed. The passwords you enter are not displayed.

```
RBT-8100# set enablepass
Enter old password: old-password
Enter new password: new-password
Retype new password: new-password
Password changed
```

Related Commands

- disable on page 2-2
- enable on page 2-3

3

System Services Commands

Use system services commands to configure and monitor system information for a RoamAbout switch. This chapter presents system services commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear banner motd	3-2
clear history	3-3
clear prompt	3-4
clear system	3-5
help	3-6
history	3-7
set auto-config	3-8
set banner motd	3-10
set confirm	3-11
set length	3-12
set license	3-13
set prompt	3-14
set system contact	3-15
set system countrycode	3-16
set system idle-timeout	3-19
set system idle-timeout	3-19
set system ip-address	3-20
set system location	3-21
set system name	3-22
show banner motd	3-23
show load	3-24
show system	3-26
show licenses	3-25
show tech-support	3-28

clear banner motd

Deletes the message-of-the-day (MOTD) banner that is displayed before the login prompt for each CLI session on the RoamAbout switch.

Syntax

```
clear banner motd
```

Defaults

None.

Mode

Enabled.

Example

To clear a banner, type the following command:

```
RBT-8100# clear banner motd
success: change accepted
```

Note: As an alternative to clearing the banner, you can overwrite the existing banner with an empty banner by typing the following command: **`set banner motd ^^`**

Related Commands

- set banner motd on page 3-10
- show banner motd on page 3-23

clear history

Deletes the command history buffer for the current CLI session.

Syntax

clear history

Defaults

None.

Mode

All.

Example

To clear the history buffer, type the following command:

```
RBT-8100# clear history
success: command buffer was flushed.
```

Related Commands

history on page 3-7

clear prompt

Resets the system prompt to its previously configured value. If the prompt was not configured previously, this command resets the prompt to its default.

Syntax

clear prompt

Defaults

None.

Mode

Enabled.

Example

To reset the prompt, type the following command:

```
wildebeest# clear prompt
success: change accepted.
RBT-8100#
```

Related Commands

set prompt on page 3-14. (For information about default prompts, see "Command Prompts" on page 1-2.)

clear system

Clears the system configuration of the specified information.

Caution: If you change the IP address, any currently configured Mobility Domain operations cease. You must reset the Mobility Domain.

Syntax

clear system [**contact** | **countrycode** | **ip-address** | **location** | **name**]

Parameters

contact	Resets the name of contact person for the RoamAbout switch to null.
countrycode	Resets the country code for the RoamAbout switch to null.
idle-timeout	Resets the number of seconds a CLI management session can remain idle to the default value (3600 seconds).
ip-address	Resets the IP address of the RoamAbout switch to null.
location	Resets the location of the RoamAbout switch to null.
name	Resets the name of the RoamAbout switch to the default system name, which is *RBT-mm-nnnnnn*, where *mm* is the model number and *nnnnnn* is the last 6 digits of the switch's MAC address.

Defaults

None.

Mode

Enabled.

Example

To clear the location of the RoamAbout switch, type the following command:

```
RBT-8100# clear system location
success: change accepted.
```

help

Displays a list of commands that can be used to configure and monitor the RoamAbout switch.

Syntax

help

Defaults

None.

Mode

All.

Example

Use this command to see a list of available commands. If you have restricted access, you see fewer commands than if you have enabled access. To display a list of CLI commands available at the enabled access level, type the following command at the enabled access level:

RBT-8100# **help**

```
Commands:
--------------------------------------------------------------------------------
clear                  Clear,  use 'clear help' for more information
commit                 Commit the content of the ACL table
copy                   Copy from filename (or url) to filename (or url)
crypto                 Crypto, use 'crypto help' for more information
delete                 Delete url
dir                    Show list of files on flash device
disable                Disable privileged mode
exit                   Exit from the Admin session
help                   Show this help screen
history                Show contents of history substitution buffer
hit-sample-rate        Set NP hit-counter sample rate
load                   Load, use 'load help' for more information
logout                 Exit from the Admin session
monitor                Monitor, use 'monitor help' for more information
ping                   Send echo packets to hosts
quit                   Exit from the Admin session
reset                  Reset, use 'reset help' for more information
rollback               Remove changes to the edited ACL table
save                   Save the running configuration to persistent storage
set                    Set, use 'set help' for more information
show                   Show, use 'show help' for more information
telnet                 telnet IP address [server port]
traceroute             Print the route packets take to network host
```

Related Commands

Using CLI Help on page 1-7

history

Displays the command history buffer for the current CLI session.

Syntax

history

Defaults

None.

Mode

All.

Example

To show the history of your session, type the following command:

```
RBT-8100> history
Show History (most recent first)
--------------------------------
[00] show config
[01] show version
[02] enable
```

Related Commands

clear history on page 3-3

set auto-config

Enables a RoamAbout switch to contact a RoamAbout Switch Manager (RASM) server for its configuration.

Syntax

```
set auto-config {enable | disable}
```

Parameters

enable	Enables the switch to contact a RASM server to request a configuration.
disable	Disables the auto-config option.

Defaults

However, auto-config is disabled by default on the RBT-8100.

Mode

Enabled.

Usage

A network administrator at the corporate office can preconfigure the switch in a RASM network plan. The switch configuration must have a name for the switch, and the serial number must match the switch's serial number. The configuration should also include all other settings required for the deployment, including access point configuration, SSIDs, AAA settings, and so on.

When the RASM server in the corporate network receives the configuration request, the server looks in the currently open network plan for a switch configuration with the same model and serial number as the one in the configuration request.

- If the network plan contains a configuration with a matching model and serial number, RASM sends the configuration to the switch and restarts the switch. The switch boots using the configuration it received from RASM.
- If the network plan does not have a configuration with a matching model and serial number, a verification warning appears in RASM. The warning lists the switch's serial number and IP address. The network administrator can upload the switch into the network plan, configure switch parameters, and deploy the configuration to the switch.

If you want a RoamAbout switch model to be able to access a RASM server for a configuration, you also must preconfigure the RoamAbout switch with the following information:

- IP address
- Default router (gateway) address
- Domain name and DNS server address

You can enable the switch to use the MSS DHCP client to obtain this information from a DHCP server in the local network where the switch will be deployed. Alternatively, you can statically configure the information.

The IP address and DNS information are configured independently. You can configure the combination of settings that work with the network resources available at the deployment site. The following examples show some of the combinations you can configure.

Example

The following commands stage an RBT-8100 switch to use the auto-config option. The network where the switch is installed has a DHCP server, so the switch is configured to use the MSS DHCP client to obtain an IP address, default router address, DNS domain name, and DNS server IP addresses.

1. Configure a VLAN:
```
RBT-8100# set vlan 1 port 7
success: change accepted.
```
2. Enable the DHCP client on VLAN 1:
```
RBT-8100# set interface 1 ip dhcp-client enable
success: change accepted.
```
3. Enable the auto-config option:
```
RBT-8100# set auto-config enable
success: change accepted.
```
4. Save the configuration changes:
```
RBT-8100# save config
success: configuration saved.
```

Related Commands

- crypto generate key on page 15-6
- crypto generate self-signedweb on page 15-9
- save config on page 20-20
- set interface dhcp-client on page 7-25
- set vlan port on page 5-12

set banner motd

Configures the banner string that is displayed before the beginning of each login prompt for each CLI session on the RoamAbout switch.

Syntax

set banner motd ^*text*^

Parameters

^	Delimiting character that begins and ends the message.
text	Up to 2000 alphanumeric characters, including tabs and carriage returns, but *not* the delimiting character (^). The maximum number of characters is approximately 24 lines by 80 characters.

Defaults

None.

Mode

Enabled.

Usage

Type a caret (^), then the message, then another caret.

Do not use the following characters with commands in which you set text to be displayed on the RoamAbout switch, such as message-of-the-day (MOTD) banners:

- Ampersand (&)
- Angle brackets (< >)
- Double quotation marks (“”)
- Number sign (#)
- Question mark (?)
- Single quotation mark (')

Example

To create a banner that says *Update meeting at 3 p.m.*, type the following command:

```
RBT-8100# set banner motd ^Update meeting at 3 p.m.^
success: change accepted.
```

Related Commands

- clear banner motd on page 3-2
- show banner motd on page 3-23

set confirm

Enables or disables the display of confirmation messages for commands that might have a large impact on the network.

Syntax

set confirm {**on** | **off**}

Parameters

on	Enables confirmation messages.
off	Disables confirmation messages.

Defaults

Configuration messages are enabled.

Mode

Enabled.

Usage

This command remains in effect for the duration of the session, until you enter an **exit** or **quit** command, or until you enter another **set confirm** command.

MSS displays a message requiring confirmation when you enter certain commands that can have a potentially large impact on the network. For example:

```
RBT-8100# clear vlan red
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]
```

Example

To turn off these confirmation messages, type the following command:

```
RBT-8100# set confirm off
success: Confirm state is off
```

set length

Defines the number of lines of CLI output to display between paging prompts. MSS displays the set number of lines and waits for you to press any key to display another set, or type **q** to quit the display.

Syntax

set length *number-of-lines*

Parameters

number-of-lines	Number of lines of text to display between paging prompts. You can specify from 0 to 512. The 0 value disables the paging prompt action entirely.

Defaults

MSS displays 24 lines by default.

Mode

All.

Usage

Use this command if the output of a CLI command is greater than the number of lines allowed by default for a terminal type.

Example

To set the number of lines displayed to 100, type the following command:

```
RBT-8100# set length 100
success: screen length for this session set to 100
```

set license

Installs an upgrade license key on an RBT-8400 or RBT-8200 switch.

The RBT-8400 or RBT-8200 switch can boot and manage up to 40 access points by default. You can increase the access point support to 80 access points or 120 access points, by installing one or two activation keys. Activation keys are available for 40 additional access points or 80 additional access points. You can install a 40-access point upgrade or an 80-access point upgrade. If you have already installed a 40-access point upgrade, you can install one additional 40-access point upgrade.

Syntax

set license *activation-key*

Parameters

activation-key	Hexadecimal digits generated by the Enterasys Networks license server or otherwise provided by Enterasys Networks for your switch. The activation key is based on the switch's serial number. You can enter the number in either of the following formats: xxxx-xxxx-xxxx-xxxx-xxxx xxxxxxxxxxxxxxxxxxxx

Defaults

None.

Mode

Enabled.

Usage

This command applies only to the RBT-8400 or RBT-8200.

Example

To install an activation key for an additional 80 access points, type the following command:

```
RBT-8400# set license 3B02-D821-6C19-CE8B-F20E
success: license accepted
```

Related Commands

show licenses on page 3-25

set prompt

Changes the CLI prompt for the RoamAbout switch to a string you specify.

Syntax

set prompt *string*

Parameters

string	Alphanumeric string up to 32 characters long. To include spaces in the prompt, you must enclose the string in double quotation marks (“”).

Defaults

The factory default for the RoamAbout switch name is *RBT-mm-nnnnnn*, where *mm* is the model number and *nnnnnn* is the last 6 digits of the 12-digit system MAC address.

Mode

Enabled.

Usage

When you first log in for the initial configuration of the RoamAbout switch, the CLI provides an *RBT-mm-nnnnnn*> prompt. After you become enabled by typing **enable** and giving a suitable password, the *RBT-mm-nnnnnn*# prompt is displayed.

If you use the **set system name** command to change the default system name, MSS uses that name in the prompt, unless you also change the prompt with **set prompt**.

Example

The following example sets the prompt from RBT-8100 to *happy_days*:

```
RBT-8100# set prompt happy_days
success: change accepted.
happy_days#
```

Related Commands

- clear prompt on page 3-4
- set system name on page 3-22
- show config on page 20-26

set system contact

Stores a contact name for the RoamAbout switch.

Syntax

set system contact *string*

Parameters

string	Alphanumeric string up to 256 characters long, with no blank spaces.

Defaults

None.

Mode

Enabled.

To view the system contact string, type the **show system** command.

Example

The following command sets the system contact information to *tamara@example.com*:

```
RBT-8100# set system contact tamara@example.com
success: change accepted.
```

Related Commands

- clear system on page 3-5
- set system location on page 3-21
- set system name on page 3-22
- show system on page 3-26

set system countrycode

Defines the country-specific IEEE 802.11 regulations to enforce on the RoamAbout switch.

Syntax

set system countrycode *code*

Parameters

code	Two-letter code for the country of operation for the RoamAbout switch. You can specify one of the codes listed in Table 3-1.

Table 3-1 Country Codes

Country	Code
Australia	**AU**
Austria	**AT**
Belgium	**BE**
Brazil	**BR**
Canada	**CA**
China	**CN**
Czech Republic	**CZ**
Denmark	**DK**
Finland	**FI**
France	**FR**
Germany	**DE**
Greece	**GR**
Hong Kong	**HK**
Hungary	**HU**
Iceland	**IS**
India	**IN**
Ireland	**IE**
Israel	**IL**
Italy	**IT**
Japan	**JP**
Liechtenstein	**LI**

Table 3-1 Country Codes (continued)

Country	Code
Luxembourg	**LU**
Malaysia	**MY**
Mexico	**MX**
Netherlands	**NL**
New Zealand	**NZ**
Norway	**NO**
Poland	**PL**
Portugal	**PT**
Saudi Arabia	**SA**
Singapore	**SG**
Slovakia	**SK**
Slovenia	**SI**
South Africa	**ZA**
South Korea	**KR**
Spain	**ES**
Sweden	**SE**
Switzerland	**CH**
Taiwan	**TW**
Thailand	**TH**
United Arab Emirates	**AE**
United Kingdom	**GB**
United States	**US**

Defaults

The factory default country code is *None*.

Mode

Enabled.

Usage

You must set the system county code to a valid value before using any **set ap** commands to configure an access point.

Example

To set the country code to Canada, type the following command:

```
RBT-8100#  set system country code CA
success: change accepted.
```

Related Commands

show config on page 20-26

set system idle-timeout

Specifies the maximum number of seconds a CLI management session with the switch can remain idle before MSS terminates the session.

Syntax

set system idle-timeout *seconds*

Parameters

seconds	Number of seconds a CLI management session can remain idle before MSS terminates the session. You can specify from 0 to 86400 seconds (one day). If you specify 0, the idle timeout is disabled. The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the CLI rounds up to the next 30-second increment. For example, if you enter 31, the CLI rounds up to 60.

Defaults

3600 seconds (one hour).

Mode

Enabled.

Usage

This command applies to all types of CLI management sessions: console, Telnet, and SSH. The timeout change applies to existing sessions only, not to new sessions.

Example

This command applies to all types of CLI management sessions: console, Telnet, and SSH. The timeout change applies to existing sessions and new sessions.

The following command sets the idle timeout to 1800 seconds (one half hour):

```
RBT-8100# set system idle-timeout 1800
success: change accepted.
```

Related Commands

- clear system on page 3-5
- show system on page 3-26

set system ip-address

Sets the system IP address so that it can be used by various services in the RoamAbout switch.

Caution: Any currently configured Mobility Domain operations cease if you change the IP address. If you change the address, you must reset the Mobility Domain.

Syntax

set system ip-address *ip-addr*

Parameters

ip-addr	IP address, in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Example

The following command sets the IP address of the RoamAbout switch to 192.168.253.1:

```
RBT-8100# set system ip-address 192.168.253.1
success: change accepted.
```

Related Commands

- clear system on page 3-5
- set interface on page 7-24
- show system on page 3-26

set system location

Stores location information for the RoamAbout switch.

Syntax

set system location *string*

Parameters

string	Alphanumeric string up to 256 characters long, with no blank spaces.

Defaults

None.

Mode

Enabled.

Usage

You cannot include spaces in the system location string.

To view the system location string, type the **show system** command.

Example

To store the location of the RoamAbout switch in the switch's configuration, type the following command:

```
RBT-8100# set system location first-floor-bldg3
success: change accepted.
```

Related Commands

- clear system on page 3-5
- set system contact on page 3-15
- set system name on page 3-22
- show system on page 3-26

set system name

Changes the name of the RoamAbout switch from the default system name and also provides content for the CLI prompt, if you do not specify a prompt.

Syntax

set system name *string*

Parameters

string	Alphanumeric string up to 256 characters long, with no blank spaces. RoamAbout Switch Manager requires unique RoamAbout switch names.

Defaults

By default, the system name and command prompt have the same value. The factory default for both is *RBT-mm-nnnnnn*, where *mm* is the model number and *nnnnnn* is the last 6 digits of the 12-digit system MAC address.

Mode

Enabled.

Usage

Entering **set system name** with no string resets the system name to the factory default.

To view the system name string, type the **show system** command.

Example

The following example sets the system name to a name that identifies the RoamAbout switch:

```
RBT-8100# set system name RBT-bldg3
success: change accepted.
RBT-bldg3#
```

Related Commands

- clear system on page 3-5
- set prompt on page 3-14
- set system contact on page 3-15
- set system location on page 3-21
- show system on page 3-26

show banner motd

Shows the banner that was configured with the **set banner motd** command.

Syntax

```
show banner motd
```

Defaults

None.

Mode

Enabled.

Example

To display the banner with the message of the day, type the following command:

```
RBT-8100# show banner motd
hello world
```

Related Commands

- clear banner motd on page 3-2
- set banner motd on page 3-10

show load

Displays CPU usage on the switch.

Syntax

show load

Defaults

None.

Mode

Enabled.

Example

To display the CPU load recorded from the time the switch was booted, as well as from the previous time the **show load** command was run, enter the following command:

```
RBT-8100# show load
System Load: overall: 2% delta: 5%
```

The overall field shows the CPU load as a percentage from the time the switch was booted. The delta field shows CPU load as a percentage from the last time the **show load** command was entered.

Related Commands

show system on page 3-26

show licenses

Displays information about the license key(s) currently installed on a RBT-8400 switch.

Syntax

show licenses

Defaults

None.

Mode

All.

Usage

This command applies only to the RBT-8200 or RBT-8400.

Example

To view RBT-8400 license keys, type the following command:

```
RBT-8400# show licenses
Feature          : 80 additional MAPs
```

Related Commands

set license on page 3-13

show system

Displays system information.

Syntax

show system

Defaults

None.

Mode

Enabled.

Example

To show system information, type the following command:

```
RBT-8100# show system
================================================================================
 Product Name:       RBT-8100
 System Name:        RBT-bldg3
 System Countrycode: US
 System Location:    first-floor-bldg3
 System Contact:     tamara@example.com
 System IP:          192.168.12.7
 System MAC:         00:0B:0E:00:04:30
================================================================================
 Boot Time:          2003-11-07 15:45:49
 Uptime:                 13 days 04:29:10
================================================================================
 Fan status:  fan1 OK fan2 OK fan3 OK
 Temperature: temp1 ok  temp2 ok  temp3 ok
 PSU Status:  Lower Power Supply DC ok AC ok  Upper Power Supply missing
 Memory:      97.04/744.03 (13%)
 Total Power Over Ethernet : 29.000
================================================================================
```

Table 3-2 describes the fields of **show system** output.

Table 3-2 show system Output

Field	Description
Product Name	RAS model number.
System Name	System name (factory default, or optionally configured with **set system name**).
System Countrycode	Country-specific 802.11 code required for AP operation (configured with **set system countrycode**).
System Location	Record of RAS's physical location (optionally configured with **set system location)**.

Table 3-2 show system Output (continued)

Field	Description
System Contact	Contact information about the system administrator or another person to contact about the system (optionally configured with **set system contact**).
System IP	Common interface, source, and default IP address for the RAS, in dotted decimal notation (configured with **set system ip-address**).
System idle timeout	Number of seconds MSS allows a CLI management session (console, Telnet, or SSH) to remain idle before terminating the session. (The system idle timeout can be configured using the **set system idle-timeout** command.)
System MAC	RAS media access control (MAC) machine address set at the factory, in 6-byte hexadecimal format.
Boot Time	Date and time of the last system reboot.
Uptime	Number of days, hours, minutes, and seconds that the RAS has been operating since its last restart.
Fan status	Operating status of the RAS cooling fans: • OK—Fan is operating. • Failed—Fan is not operating. MSS sends an alert to the system log every 5 minutes until this condition is corrected.
Temperature	Status of temperature sensors at three locations in the RAS: • ok—Temperature is within the acceptable range of 0° C to 50° C (32° F to 122° F). • Alarm—Temperature is above or below the acceptable range. MSS sends an alert to the system log every 5 minutes until this condition is corrected.
PSU Status	Status of the lower and upper power supply units: • missing—Power supply is not installed or is inoperable. • DC ok—Power supply is producing DC power. • DC output failure—Power supply is not producing DC power. MSS sends an alert to the system log every 5 minutes until this condition is corrected. • AC ok—Power supply is receiving AC power. • AC not present—Power supply is not receiving AC power.
Memory	Current size (in megabytes) of nonvolatile memory (NVRAM) and synchronous dynamic RAM (SDRAM), plus the percentage of total memory space in use, in the following format: *NVRAM size ISDRAM size* (*percent of total*)

Related Commands

- clear system on page 3-5
- set system contact on page 3-15
- set system countrycode on page 3-16
- set system ip-address on page 3-20
- set system location on page 3-21
- set system name on page 3-22

show tech-support

Provides an in-depth snapshot of the status of the RoamAbout switch, which includes details about the boot image, the version, ports, and other configuration values. This command also displays the last 100 log messages.

Syntax

show tech-support [**file** [*subdirname/*]*filename*]

Parameters

[*subdirname/*]*filename*	Optional subdirectory name, and a string up to 32 alphanumeric characters. The command's output is saved into a file with the specified name in nonvolatile storage.

Defaults

None.

Mode

Enabled.

Usage

Enter this command before calling the Enterasys Networks Global Technical Assistance Center (GTAC). See "Getting Help" on page xxiii for more information.

Related Commands

- show boot on page 20-24
- show config on page 20-26
- show licenses on page 3-25
- show system on page 3-26
- show version on page 20-28

4

Port Commands

Use port commands to configure and manage individual ports and load-sharing port groups. This chapter presents port commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear dap	4-2
clear port counters	4-3
clear port-group	4-4
clear port media-type	4-5
clear port mirror	4-6
clear port name	4-7
clear port type	4-8
monitor port counters	4-10
reset port	4-14
set dap	4-15
set port	4-17
set port-group	4-18
set port media-type	4-20
set port mirror	4-20
set port name	4-21
set port negotiation	4-22
set port speed	4-24
set port speed	4-24
set port speed	4-24
set port trap	4-25
set port type wired-auth	4-26
show port counters	4-28
show port-group	4-29
show port media-type	4-30
show port status	4-31

clear dap

Caution: When you clear a Distributed access point, MSS ends user sessions that are using the access point.

Removes a Distributed Access Point (DAP).

Syntax

clear dap *dap-num*

Parameters

dap-num	Number of the Distributed access point(s) you want to remove.

Defaults

None.

Mode

Enabled.

Example

The following command clears Distributed access point 1:

```
RBT-8100# clear dap 1
This will clear specified DAP devices. Would you like to continue? (y/n) [n]y
```

Related Commands

set dap on page 4-15

clear port counters

Clears port statistics counters and resets them to 0.

Syntax

```
clear port counters
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following command clears all port statistics counters and resets them to 0:

```
RBT-8100# clear port counters
success: cleared port counters
```

Related Commands

- monitor port counters on page 4-10
- show port counters on page 4-28

clear port-group

Removes a port group.

Syntax

clear port-group name *name*

Parameters

name *name*	Name of the port group.

Defaults

None.

Mode

Enabled.

Example

The following command clears port group *server1*:

```
RBT-8100# clear port-group name server1
success: change accepted.
```

Related Commands

- set port-group on page 4-18
- show port-group on page 4-29

clear port media-type

Disables the copper interface and re-enables the fiber interface on an RBT-8400 gigabit Ethernet port.

Syntax

clear port media-type *port-list*

Parameters

port-list	List of physical ports. MSS disables the copper interface and re-enables the fiber interface on all the specified ports.

Defaults

The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Mode

Enabled.

Usage

This command applies only to the RBT-8400. This command does not affect a link that is already active on the port.

Example

The following command disables the copper interface and re-enables the fiber interface on port 2:

```
RBT-8400# clear port media-type 2
```

Related Commands

- set port media-type on page 4-19
- show port media-type on page 4-30

clear port mirror

Removes a port mirroring configuration.

Syntax

clear port mirror

Defaults

None.

Mode

Enabled.

Examples

The following command clears the port mirroring configuration from the switch:

```
RBT-8100# clear port mirror
```

Related Commands

- set port mirror on page 4-20
- set port mirror on page 4-20

clear port name

Removes the name assigned to a port.

Syntax

clear port *port-list* **name**

Parameters

port-list ***name***	List of physical ports. MSS removes the names from all the specified ports.

Defaults

None.

Mode

Enabled.

Examples

The following command clears the names of ports 17 through 20:

```
RBT-8100# clear port 17-20 name
```

The following command removes the names from ports 1 and 3 through 5:

Related Commands

- set port name on page 4-21
- show port status on page 4-31

clear port type

Note: When you clear a port, MSS ends user sessions that are using the port.

Removes all configuration settings from a port and resets the port as a network port.

Syntax

clear port type *port-list*

Parameters

port-list	List of physical ports. MSS resets and removes the configuration from all the specified ports.

Defaults

The cleared port becomes a network port but is not placed in any VLANs.

Mode

Enabled.

Usage

Use this command to change a port back to a network port. All configuration settings specific to the port type are removed. For example, if you clear an Access Point port, all AP-specific settings are removed. Table 4-1 lists the default network port settings that MSS applies when you clear a port's type.

Table 4-1 Network Port Defaults

Port Parameter	Setting
VLAN membership	None. **Note:** Although the command changes a port to a network port, the command does not place the port in any VLAN. To use the port in a VLAN, you must add the port to the VLAN.
Spanning Tree Protocol (STP)	Based on the VLAN(s) you add the port to.
802.1X	No authorization.
Port groups	None.
Internet Group Management Protocol (IGMP) snooping	Enabled as port is added to VLANs.
Access Point and radio parameters	Not applicable
Maximum user sessions	Not applicable

Example

The following command clears port 5:

```
RBT-8100# clear port type 5
This may disrupt currently authenticated users. Are you sure? (y/n) [n]y
success: change accepted.
```

Related Commands

set port type wired-auth on page 4-26

monitor port counters

Displays and continually updates port statistics.

Syntax

```
monitor port counters [octets | packets | receive-errors | transmit-errors |
collisions | receive-etherstats | transmit-etherstats]
```

Parameters

octets	Displays octet statistics first.
packets	Displays packet statistics first.
receive-errors	Displays errors in received packets first.
transmit-errors	Displays errors in transmitted packets first.
collisions	Displays collision statistics first.
receive-etherstats	Displays Ethernet statistics for received packets first.
transmit-etherstats	Displays Ethernet statistics for transmitted packets first.

Defaults

All types of statistics are displayed for all ports. MSS refreshes the statistics every 5 seconds. This interval cannot be configured. Statistics types are displayed in the following order by default:

- Octets
- Packets
- Receive errors
- Transmit errors
- Collisions
- Receive Ethernet statistics
- Transmit Ethernet statistics

Mode

All.

Usage

Each type of statistic is displayed separately. Press the Spacebar to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed in Table 4-2 to control the monitor display.

Table 4-2 Key Controls for Monitor Port Counters Display

Key	Effect on Monitor Display
Spacebar	Advances to the next statistic type.

Table 4-2 Key Controls for Monitor Port Counters Display (continued)

Key	Effect on Monitor Display
Esc	Exits the monitor. MSS stops displaying the statistics and displays a new command prompt.
c	Clears the statistics counters for the currently displayed statistics type. The counters begin incrementing again.

For error reporting, the cyclic redundancy check (CRC) errors include misalignment errors. Jumbo packets with valid CRCs are not counted. A short packet can be reported as a short packet, a CRC error, or an overrun. In some circumstances, the transmitted octets counter might increment a small amount for a port with nothing attached.

Example

The following command starts the port statistics monitor beginning with octet statistics (the default):

```
RBT-8100# monitor port counters
```

As soon as you press Enter, MSS clears the window and displays statistics at the top of the window.

```
Port   Status                       Rx Octets                          Tx Octets
================================================================================
    1  Up                          27965420                          34886544
...
```

To cycle the display to the next set of statistics, press the Spacebar. In this example, packet statistics are displayed next:

```
Port   Status     Rx Unicast    Rx NonUnicast       Tx Unicast     Tx NonUnicast
================================================================================
    1  Up            54620           62144           68318            62556
...
```

Table 4-3 on page 4-12 describes the port statistics displayed by each statistics option. The Port and Status fields are displayed for each option.

Table 4-3 Output for Monitor Port Counters

Statistics Option	Field	Description
Displayed for All Options	Port	Port the statistics are displayed for.
	Status	Port status. The status can be Up or Down.
octets	Rx Octets	Total number of octets received by the port. This number includes octets received in frames that contained errors.
	Tx Octets	Total number of octets received. This number includes octets received in frames that contained errors.
packets	Rx Unicast	Number of unicast packets received. This number does not include packets that contain errors.
	Rx NonUnicast	Number of broadcast and multicast packets received. This number does not include packets that contain errors.
	Tx Unicast	Number of unicast packets transmitted. This number does not include packets that contain errors.
	Tx NonUnicast	Number of broadcast and multicast packets transmitted. This number does not include packets that contain errors.
receive-errors	Rx Crc	Number of frames received by the port that had the correct length but contained an invalid frame check sequence (FCS) value. This statistic includes frames with misalignment errors.
	Rx Error	Total number of frames received in which the Physical layer (PHY) detected an error.
	Rx Short	Number of frames received by the port that were fewer than 64 bytes long.
	Rx Overrun	Number of frames received by the port that were valid but were longer than 1518 bytes. This statistic does not include jumbo packets with valid CRCs.
transmit-errors	Tx Crc	Number of frames transmitted by the port that had the correct length but contained an invalid FCS value.
	Tx Short	Number of frames transmitted by the port that were fewer than 64 bytes long.
	Tx Fragment	Total number of frames transmitted that were less than 64 octets long and had invalid CRCs.
	Tx Abort	Total number of frames that had a link pointer parity error.

Table 4-3 Output for Monitor Port Counters (continued)

Statistics Option	Field	Description
collisions	Single Coll	Total number of frames transmitted that experienced one collision before 64 bytes of the frame were transmitted on the network.
	Multiple Coll	Total number of frames transmitted that experienced more than one collision before 64 bytes of the frame were transmitted on the network.
	Excessive Coll	Total number of frames that experienced more than 16 collisions during transmit attempts. These frames are dropped and not transmitted.
	Total Coll	Best estimate of the total number of collisions on this Ethernet segment.
receive-etherstats	Rx 64	Number of packets received that were 64 bytes long.
	Rx 127	Number of packets received that were from 65 through 127 bytes long.
	Rx 255	Number of packets received that were from 128 through 255 bytes long.
	Rx 511	Number of packets received that were from 256 through 511 bytes long.
	Rx 1023	Number of packets received that were from 512 through 1023 bytes long.
	Rx 1518	Number of packets received that were from 1024 through 1518 bytes long.
transmit-etherstats	Tx 64	Number of packets transmitted that were 64 bytes long.
	Tx 127	Number of packets transmitted that were from 65 through 127 bytes long.
	Tx 255	Number of packets transmitted that were from 128 through 255 bytes long.
	Tx 511	Number of packets transmitted that were from 256 through 511 bytes long.
	Tx 1023	Number of packets transmitted that were from 512 through 1023 bytes long.
	Tx 1518	Number of packets transmitted that were from 1024 through 1518 bytes long.

Related Commands

show port counters on page 4-28

reset port

Resets a port by toggling its link state and Power over Ethernet (PoE) state.

Syntax

reset port *port-list*

Parameters

port-list	List of physical ports. MSS resets all the specified ports.

Defaults

None.

Mode

Enabled.

Usage

The **reset** command disables the port's link and PoE (if applicable) for at least 1 second, then reenables them. This behavior is useful for forcing an Access Point that is connected to two RoamAbout switches to reboot over the link to the other switch.

Example

The following command resets port 5:

```
RBT-8100# reset port 5
<<no cli response>>
```

Related Commands

set port on page 4-17

set dap

Configures a Distributed access point for an Access Point that is indirectly connected to the RoamAbout switch through an intermediate Layer 2 or Layer 3 network.

Notes: Before configuring a Distributed access point, you must use the **set system countrycode** command to set the IEEE 802.11 country-specific regulations on the RoamAbout switch. See set system countrycode on page 3-16.

Syntax

set dap *dap-num* **serial-id** *serial-ID* **model** {**AP3000**} [**radiotype** {**11a** | **11b**| **11g**}]

Parameters

dap-num	Number for the Distributed access point. The range of valid connection numbers depends on the RoamAbout switch model: • For an RBT-8400, you can specify a number from 1 to 20.
serial-id *serial-ID*	Access point serial ID. The serial ID is listed on the access point case. To display the serial ID using the CLI, use the **show version details** command.
model {**AP3000**}	Access point model.
radiotype 11a | **11b**| **11g**	Radio type: • **11a**—802.11a • **11b**—802.11b • **11g**—802.11g **Note:** This option applies only to single-radio models.

Defaults

The default radio type for model AP3000 is 802.11g.

Access point radios configured for 802.11g also allow associations from 802.11b clients by default. To disable support for 802.11b associations, use the **set radio-profile 11g-only** command on the radio profile that contains the radio.

Access point-3*xx* models have an internal 802.1b/g antenna as well as a connector for an external antenna, so use of an external antenna is optional on these models. The RBT-1602 also has a connector for an optional external 802.11a antenna. To specify the antenna model, use the **set {ap | dap} radio antennatype** command.

Mode

Enabled.

Example

The following command configures Distributed access point 1 for access point model RBT-1602 with serial-ID 0322199999:

```
RBT-8100# set dap 1 serial-id 0322199999 model RBT-1602
success: change accepted.
```

The following command removes Distributed access point 1:

```
RBT-8100# clear dap 1
This will clear specified DAP devices. Would you like to continue? (y/n) [n]y
```

Related Commands

- clear dap on page 4-2
- clear port type on page 4-8
- set port type wired-auth on page 4-26
- set system countrycode on page 3-16

set port

Administratively disables or reenables a port.

Syntax

set port {**enable** | **disable**} *port-list*

Parameters

enable	Enables the specified ports.
disable	Disables the specified ports.
port-list	List of physical ports. MSS disables or re-enables all the specified ports.

Defaults

All ports are enabled.

Mode

Enabled.

Usage

A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

Example

The following command disables port 16:

```
RBT-8100# set port disable 16
success: set "disable" on port 16
```

The fol1owing command reenables the port:

```
RBT-8100# set port enable 16
success: set "enable" on port 16
```

Related Commands

reset port on page 4-11

set port-group

Configures a load-sharing port group. All ports in the group function as a single logical link.

Syntax

set port-group name *group-name port-list* **mode** {**on** | **off**}

Parameters

name *group-name*	Alphanumeric string of up to 255 characters, with no spaces.
port-list	List of physical ports. All the ports you specify are configured together as a single logical link.
mode {**on** | **off**}	State of the group. Use **on** to enable the group or **off** to disable the group. The group is enabled by default.

Defaults

Once configured, a group is enabled by default.

Mode

Enabled.

Usage

You can configure up to 16 ports in a port group, in any combination of ports. The port numbers do not need to be contiguous and you can use 10/100 Ethernet ports and gigabit Ethernet ports in the same port group.

After you add a port to a port group, you cannot configure port parameters on the individual port. Instead, change port parameters on the entire group. Specify the group name instead of an individual port name or number in port configuration commands.

To add or remove ports in a group that is already configured, change the mode to **off**, add or remove the ports, then change the mode to **on**.

Example

The following command configures a port group named *server1* containing ports 1 through 5, and enables the link:

```
RBT-8100# set port-group name server1 1-5 mode on
success: change accepted.
```

The following commands disable the link for port group *server1*, change the list of ports in the group, and re-enable the link:

```
RBT-8100# set port-group name server1 1-5 mode off
success: change accepted.
RBT-8100# set port-group name server1 1-4,7 mode on
success: change accepted.
```

Related Commands

- clear port-group on page 4-3
- show port-group on page 4-29

set port media-type

Disables the fiber interface and enables the copper interface on an RBT-8400 gigabit Ethernet port.

Syntax

set port media-type *port-list* **rj45**

Parameters

port-list	List of physical ports. MSS sets the preference on all the specified ports.
rj45	Uses the copper interface.

Defaults

The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Mode

Enabled.

UsageThis command applies only to the RBT-8400.

If you set the port interface to RJ-45 on a port that already has an active fiber link, MSS immediately changes the link to the copper interface.

Example

The following command disables the fiber interface and enables the copper interface on port 2:

```
RBT-8400# set port media-type 2 rj45
```

Related Commands

- clear port media-type on page 4-5
- show port media-type on page 4-30

set port mirror

Configures port mirroring. Port mirroring is a troubleshooting feature that copies (mirrors) traffic sent or received by an RoamAbout Switch port (the source port) to another port (the observer) on the same RoamAbout Switch. You can attach a protocol analyzer to the observer port to examine the source port's traffic. Both traffic directions (send and receive) are mirrored.

Syntax

set port mirror *source-port* **observer** *observer-port*

source-port	Number of the port whose traffic you want to analyze. You can specify only one port.
observer-port	Number of the port to which you want the switch to copy the source port's traffic.

Defaults

None.

Mode

Enabled.

Usage

The switch can have one port mirroring pair (one source port and one observer port) at a time. The source port can be a network port, RoamAbout access port, or wired authentication port. However, the observer port must be a network port, and cannot be a member of any VLAN or port group.

Example

The following command sets port 2 to monitor port 1's traffic:

```
RBT-8100# set port 1 observer 2
```

Related Commands

- clear port mirror on page 4-6

set port name

Assigns a name to a port. After naming a port, you can use the port name or number in other CLI commands.

Syntax

set port *port* **name** *name*

Parameters

port	Number of a physical port. You can specify only one port.
name *name*	Alphanumeric string of up to 16 characters, with no spaces.

Defaults

None.

Mode

Enabled.

Usage

To simplify configuration and avoid confusion between a port's number and its name, Enterasys Networks recommends that you do not use numbers as port names.

Example

The following command sets the name of port 17 to *adminpool*:

```
RBT-8100# set port 17 name adminpool
success: change accepted.
```

Example

The following command assigns the name *techpubs* to port 5:

Related Commands

- clear port name on page 4-4
- show port status on page 4-32

set port negotiation

Disables or reenables autonegotiation on gigabit Ethernet or 10/100 Ethernet ports.

Syntax

set port negotiation *port-list* {**enable** | **disable**}

Parameters

port-list	List of physical ports. MSS disables or reenables autonegotiation on all the specified ports.
enable	Enables autonegotiation on the specified ports.
disable	Disables autonegotiation on the specified ports.

Defaults

Autonegotiation is enabled on all Ethernet ports by default.

Mode

Enabled.

Usage

The gigabit Ethernet ports operate at 1000 Mbps only. They do not change speed to match 10-Mbps or 100-Mbps links.

RBT-8100 10/100 Ethernet ports do not support half-duplex operation. As a result, there are restrictions when RBT-8100 10/100 Ethernet ports are interoperating with other vendors' devices. For a link to occur, the autonegotiation settings on an RBT-8100 port and the device at the other end of the link must be the same. In addition, the other device must support full-duplex operation. When autonegotiation is enabled on an RBT-8100 port, the port advertises support for full-duplex mode only. Table 4-4 on page 4-22 lists the supported configurations.

Table 4-4 Supported 10/100 Ethernet Speeds and Operating Modes for RBT-8100

		RBT-8100 Setting		
		100 Mbps Full-duplex	**10 Mbps Full-duplex**	**Autonegotiation**
	100 Mbps Full-duplex	100 Mbps full-duplex	Not supported	Not supported
	10 Mbps Full-duplex	Not supported	10 Mbps full-duplex	Not supported
Other Device's Setting	**100 Mbps Half-duplex**	Not supported	Not supported	Not supported
	10 Mbps Half-duplex	Not supported	Not supported	Not supported
	Autonegotiation	Not supported	Not supported	100 Mbps full-duplex

Enterasys Networks recommends that you do not configure the mode of a RoamAbout Switch port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to a RoamAbout Switch port in such a configuration can cause forwarding on the link to stop.

Examples

The following command disables autonegotiation on ports 3, 8, and 16 through 18:

```
RBT-8100# set port negotiation 3,8,16-18 disable
```

The following command enables autonegotiation on port 21:

```
RBT-8100# set port negotiation 21 enable
<<no cli response>>
```

set port speed

Changes the speed of a port.

Syntax

set port speed *port-list* {**10** | **100** | **1000** | **auto**}

Parameters

port-list	List of physical ports. MSS sets the port speed on all the specified ports.
10	Sets the port speed of a 10/100 Ethernet port to 10 Mbps and sets the operating mode to full-duplex.
100	Sets the port speed of a 10/100 Ethernet port to 100 Mbps and sets the operating mode to full-duplex.
1000	Sets the port speed of a gigabit Ethernet port to 1000 Mbps and sets the operating mode to full-duplex.
auto	Enables a port to detect the speed and operating mode of the traffic on the link and set itself accordingly.

Defaults

All ports are set to **auto**.

Mode

Enabled.

Usage

Enterasys Networks recommends that you do not configure the mode of a RoamAbout Switch port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to a RoamAbout Switch port in such a configuration can cause forwarding on the link to stop.

Do not set the port speed of a gigabit port to **auto**. Although the CLI allows this setting, it is invalid. If you set the port speed of a gigabit port to **auto**, the link will stop working.

Example

The following command sets the port speed on ports 1, 7 through 11, and 14 to 10 Mbps and sets the operating mode to full-duplex:

```
RBT-8100# set port speed 1,7-11,14 10
```

set port trap

Enables or disables Simple Network Management Protocol (SNMP) linkup and linkdown traps on an individual port.

Syntax

set port trap *port-list* {**enable** | **disable**}

Parameters

port-list	List of physical ports.
enable	Enables the Telnet server.
disable	Disables the Telnet server.

Defaults

SNMP linkup and linkdown traps are disabled by default.

Mode

Enabled.

Usage

The **set port trap** command overrides the global setting of the **set snmp trap** command.

The **set port type** command does not affect the global trap information displayed by the **show snmp configuration** command. For example, if you globally enable linkup and linkdown traps but then disable the traps on a single port, the **show snmp configuration** command still indicates that the traps are globally enabled.

Example

The following command enables SNMP linkup and linkdown traps on ports 17 and 18:

```
RBT-8100# set port trap 17-18 enable
```

Related Commands

- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp trap on page 7-58
- set snmp trap receiver on page 7-59
- show snmp configuration on page 7-87

set port type wired-auth

Configures a RoamAbout switch port for a wired authentication user.

Note: Before changing the port type from **ap** to **wired-auth** or from **wired-auth** to **ap**, you must reset the port with the **clear port type** command.

Syntax

set port type wired-auth *port-list* [**tag** *tag-list*] [**max-sessions** *num*] [**auth-fall-thru** {**last-resort** | **none** }]

Parameters

port-list	List of physical ports.
tag-list	One or more numbers between 1 and 4094 that subdivide a wired authentication port into virtual ports.
num	Maximum number of simultaneous user sessions supported.
last-resort	Automatically authenticates the user, without requiring a username and password.
none	Denies authentication and prohibits the user from accessing the network over this port.
web-portal	Serves the user a web page from the RoamAbout Switch's nonvolatile storage for secure login to the network.

Defaults

The default tag-list is null (no tag values). The default number of sessions is 1. The default fallthru authentication type is **none**.

Mode

Enabled.

Usage

You cannot set a port's type if the port is a member of a port VLAN. To remove a port from a VLAN, use the **clear vlan** command. To reset a port as a network port, use the **clear port type** command.

When you change port type, MSS applies default settings appropriate for the port type. Table 4-5 lists the default settings that MSS applies when you set a port's type to **ap**.

Table 4-5 Wired Authentication Port Defaults

Port Parameter	Setting
VLAN membership	Removed from all VLANs. You cannot assign an AP access port to a VLAN. MSS automatically assigns AP access ports to VLANs based on user traffic.
Spanning Tree Protocol (STP)	Not applicable
802.1X	Uses authentication parameters configured for users.
Port groups	Not applicable

Table 4-5 Wired Authentication Port Defaults (continued)

Port Parameter	Setting
IGMP snooping	Enabled as users are authenticated and join VLANs.
Maximum user sessions	1 (one).
Fallthru authentication type	None.

Examples

The following command sets port 2for a wired authentication user:

```
RBT-8100# set port type wired-auth 2
success: change accepted
```

The following command sets port 2 for a wired authentication user and specifies a maximum of three simultaneous user sessions:

```
RBT-8100# set port type wired-auth 2 max-sessions 3
success: change accepted
```

Related Commands

clear port type on page 4-8

show port counters

Displays port statistics.

Syntax

show port counters [**octets** | **packets** | ***receive-errors*** | **transmit-errors** | **collisions** | **receive-etherstats** | **transmit-etherstats**] [**port** *port-list*]

Parameters

octets	Displays octet statistics.
packets	Displays packet statistics.
receive-errors	Displays errors in received packets.
transmit-errors	Displays errors in transmitted packets.
collisions	Displays collision statistics.
receive-etherstats	Displays Ethernet statistics for received packets.
transmit-etherstats	Displays Ethernet statistics for transmitted packets.
port *port-list*	List of physical ports. If you do not specify a port list, MSS displays statistics for all ports.

Defaults

None.

Mode

All.

Usage

You can specify one statistic type with the command.

Example

The following command shows octet statistics for port 3:

```
RBT-8100> show port counters octets port 3
Port   Status                   Rx Octets                      Tx Octets
================================================================================
    1    Up                       27965420                       34886544
```

This command's output has the same fields as the **monitor port counters** command. For descriptions of the fields, see Table 4-3 on page 9.

Related Commands

- clear port counters on page 4-3
- monitor port counters on page 4-10

show port-group

Displays port group information.

Syntax

show port-group [**all** | **name** *group-name*]

Parameters

all	Displays information for all port groups.
name *group-name*	Displays information for the specified port group.

Defaults

None.

Mode

All.

Example

The following command displays the configuration of port group *server2*:

```
RBT-8100# show port-group name server2
Port group: server2 is up
        Ports:  15, 17
```

Table 4-6 describes the fields in the **show port-group** output.

Table 4-6 Output for show port-group

Output	What It Displays...
Port group	Name and state (enabled or disabled) of the port group.
Ports	Ports contained in the port group.

Related Commands

- clear port-group on page 4-4
- set port-group on page 4-18

show port media-type

Displays the enabled interface types on an RBT-8400 switch's gigabit Ethernet ports.

Syntax

show port media-type [*port-list*]

Parameters

port-list	List of physical ports. MSS displays the enabled interface types for all the specified ports.

Defaults

None.

Mode

All.

Usage

This command applies only to the RBT-8400.

Example

The following command displays the enabled interface types on all four ports of an RBT-8400 switch:

```
RBT-8400# show port media-type
Port  Media Type
============================================================
   1  GBIC
   2  RJ45
   3  GBIC
   4  GBIC
```

Table 4-7 describes the fields in this display.

Table 4-7 Output for show port media-type

Field	Description
Port	Port number.
Preference	Preference setting: • GBIC—The GBIC (fiber) interface is enabled. • RJ45—The RJ-45 (copper) interface is enabled.

Related Commands

- clear port media-type on page 4-5
- set port media-type on page 4-19

show port status

Displays configuration and status information for ports.

Syntax

show port status [*port-list*]

Parameters

port-list	List of physical ports. If you do not specify a port list, information is displayed for all ports.

Defaults

None.

Mode

All.

Example

The following command displays information for all ports on a 22-port RoamAbout switch:

```
RBT-8100# show port status
Port  Name            Admin  Oper   Config     Actual    Type        Media
================================================================================
   1  1               up     up     auto       100/full  network     10/100BaseTx
   2  2               up     down   auto                 network     10/100BaseTx
   3  3               up     down   auto                 network     10/100BaseTx
   4  4               up     down   auto                 network     10/100BaseTx
   5  5               up     down   auto                 network     10/100BaseTx
   6  6               up     down   auto                 network     10/100BaseTx
   7  7               up     down   auto                 network     10/100BaseTx
   8  8               up     down   auto                 network     10/100BaseTx
   9  9               up     up     auto       100/full  ap          10/100BaseTx
  10  10              up     up     auto       100/full  network     10/100BaseTx
  11  11              up     down   auto                 network     10/100BaseTx
  12  12              up     down   auto                 network     10/100BaseTx
  13  13              up     down   auto                 network     10/100BaseTx
  14  14              up     down   auto                 network     10/100BaseTx
  15  15              up     down   auto                 network     10/100BaseTx
  16  16              up     down   auto                 network     10/100BaseTx
  17  17              up     down   auto                 network     10/100BaseTx
  18  18              up     down   auto                 network     10/100BaseTx
  19  19              up     down   auto                 network     10/100BaseTx
  20  20              up     down   auto                 network     10/100BaseTx
  21  21              up     down   auto                 network     no connector
  22  22              up     down   auto                 network     no connector
```

Table 4-8 describes the fields in this display.

Table 4-8 Output for show port status

Output	What It Displays...
Port	Port number.
Name	Port name. If the port does not have a name, the port number is listed.
Admin	Administrative status of the port: up—The port is enabled. down—The port is disabled.
Oper	Operational status of the port: up—The port is operational. down—The port is not operational.
Config	Port speed configured on the port: 10—10 Mbps. 100—100 Mbps. 1000—1000 Mbps. auto—The port sets its own speed.
Actual	Speed and operating mode in effect on the port.
Type	Port type: access point — Access Point port network—Network port wa—Wired authentication port
Media	Link type: 10/100BaseTX—10/100BASE-T. GBIC—1000BASE-SX or 1000BASE-LX GBIC. 1000BaseT—1000BASE-T. No connector—GBIC slot is empty.

Related Commands

- clear port type on page 4-8
- set port on page 4-17
- set port name on page 4-21
- set port negotiation on page 4-22
- set port speed on page 4-24
- set port type wired-auth on page 4-26

5

VLAN Commands

Use virtual LAN (VLAN) commands to configure and manage parameters for individual port VLANs on network ports, and to display information about clients roaming within a Mobility Domain. This chapter presents VLAN commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear fdb	5-2
clear security l2-restrict	5-4
clear security l2-restrict counters	5-5
clear vlan	5-6
set fdb	5-8
set fdb agingtime	5-9
set security l2-restrict	5-10
set vlan name	5-11
set vlan port	5-12
set vlan tunnel-affinity	5-13
show fdb	5-14
show fdb agingtime	5-16
show fdb count	5-17
show roaming station	5-18
show roaming vlan	5-20
show security l2-restrict	5-21
show tunnel	5-23
show vlan config	5-24

clear fdb

Deletes an entry from the forwarding database (FDB).

Syntax

clear fdb {**perm** | **static** | **dynamic** | **port** *port-list*} [**vlan** *vlan-id*] [**tag** *tag-value*]

Parameters

perm	Clears permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
static	Clears static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
dynamic	Clears dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle. You are not required to specify a VLAN name or number with this option.
port *port-list*	Clears dynamic entries that match destination ports in the port list. You are not required to specify a VLAN name or number with this option.
vlan *vlan-id*	VLAN name or number—required for removing permanent and static entries. For dynamic entries, specifying a VLAN removes entries that match only that VLAN. Otherwise, dynamic entries that match all VLANs are removed.
tag *tag-value*	VLAN tag value that identifies a virtual port. If you do not specify a tag value, MSS deletes only entries that match untagged interfaces. Specifying a tag value deletes entries that match only the specified tagged interface.

Defaults

None.

Mode

Enabled.

Usage

You can delete forwarding database entries based on entry type, port, or VLAN. A VLAN name or number is required for deleting permanent or static entries.

Examples

The following command clears all static forwarding database entries that match VLAN *blue*:

```
RBT-8100# clear fdb static vlan blue
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match all VLANs:

```
RBT-8100# clear fdb dynamic
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match ports 3 and 5:

```
RBT-8100# clear fdb port 3,5
success: change accepted.
```

Related Commands

- set fdb on page 5-8
- show fdb on page 5-14

clear security l2-restrict

Removes one or more MAC addresses from the list of destination MAC addresses to which clients in a VLAN are allowed to send traffic at Layer 2.

Syntax

clear security l2-restrict vlan *vlan-id* [**permit-mac** *mac-addr* [*mac-addr*] | **all**]

Parameters

vlan-id	VLAN name or number.
permit-mac *mac-addr* [*mac-addr*]	List of MAC addresses. MSS no longer allows clients in the VLAN to send traffic to the MAC addresses at Layer 2.
all	Removes all MAC addresses from the list.

If you do not specify a list of MAC addresses or **all**, all addresses are removed.

Mode

Enabled.

Usage

If you clear all MAC addresses, Layer 2 forwarding is no longer restricted in the VLAN. Clients within the VLAN will be able to communicate directly.

There can be a slight delay before functions such as pinging between clients become available again after Layer 2 restrictions are lifted. Even though packets are passed immediately once Layer 2 restrictions are gone, it can take 10 seconds or more for upper-layer protocols to update their ARP caches and regain their functionality.

To clear the statistics counters without removing any MAC addresses, use the **clear security l2-restrict counters** command instead.

Example

The following command removes MAC address aa:bb:cc:dd:ee:ff from the list of addresses to which clients in VLAN *abc_air* are allowed to send traffic at Layer 2:

```
RBT-8100# clear security l2-restrict vlan abc_air permit-mac
aa:bb:cc:dd:ee:ff
success: change accepted.
```

clear security l2-restrict counters

Clear statistics counters for Layer 2 forwarding restriction.

Syntax

clear security l2-restrict counters [**vlan** *vlan-id* | **all**]

Parameters

vlan-id	VLAN name or number.
all	Clears Layer 2 forwarding restriction counters for all VLANs.

Defaults

If you do not specify a VLAN or **all**, counters for all VLANs are cleared.

Mode

Enabled.

To clear MAC addresses from the list of addresses to which clients are allowed to send data, use the **clear security l2-restrict** command instead.

Example

The following command clears Layer 2 forwarding restriction statistics for VLAN *abc_air*:

```
RBT-8100# clear security l2-restrict counters vlan abc_air
success: change accepted.
```

clear vlan

Removes physical or virtual ports from a VLAN or removes a VLAN entirely.

Caution: When you remove a VLAN, MSS completely removes the VLAN from the configuration and also removes all configuration information that uses the VLAN. If you want to remove only a specific port from the VLAN, make sure you specify the port number in the command.

Syntax

clear vlan *vlan-id* [**port** *port-list* [**tag** *tag-value*]]

Parameters

vlan-id	VLAN name or number.
port *port-list*	List of physical ports. MSS removes the specified ports from the VLAN. If you do not specify a list of ports, MSS removes the VLAN entirely.
tag *tag-value*	Tag number that identifies a virtual port. MSS removes only the specified virtual port from the specified physical ports.

Defaults

None.

Mode

Enabled.

Usage

If you do not specify a *port-list*, the entire VLAN is removed from the configuration.

Note: You cannot delete the default VLAN but you can remove ports from it. To remove ports from the default VLAN, use the **port** *port-list* option.

Examples

The following command removes port 1 from VLAN *green*:

```
RBT-8100# clear vlan green port 1
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command removes port 4, which uses tag value 69, from VLAN *red*:

```
RBT-8100# clear vlan red port 4 tag 69
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command completely removes VLAN *marigold*:

```
RBT-8100# clear vlan marigold
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

Related Commands

- set vlan port on page 5-12
- show vlan config on page 5-24

set fdb

Adds a permanent or static entry to the forwarding database.

Syntax

set fdb {**perm** | **static**} *mac-addr* **port** *port-list* **vlan** *vlan-id* [**tag** *tag-value*]

Parameters

perm	Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Adds a static entry. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
mac-addr	Destination MAC address of the entry. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port *port-list*	List of physical destination ports for which to add the entry. A separate entry is added for each port you specify.
vlan *vlan-id*	Name or number of a VLAN of which the port is a member. The entry is added only for the specified VLAN.
tag *tag-value*	VLAN tag value that identifies a virtual port. You can specify a number from 1 through 4093. If you do not specify a tag value, an entry is created for an untagged interface only. If you specify a tag value, an entry is created only for the specified tagged interface.

Defaults

None.

Mode

Enabled.

Usage

You cannot add a multicast or broadcast address as a permanent or static FDB entry.

Example

The following command adds a permanent entry for MAC address 00:11:22:aa:bb:cc on ports 3 and 5 in VLAN *blue*:

```
RBT-8100# set fdb perm 00:11:22:aa:bb:cc port 3,5 vlan blue
success: change accepted.
```

The following command adds a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the *default* VLAN:

```
RBT-8100# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
```

Related Commands

- clear fdb on page 5-2
- show fdb on page 5-14

set fdb agingtime

Changes the aging timeout period for dynamic entries in the forwarding database.

Syntax

set fdb agingtime *vlan-id* **age** *seconds*

Parameters

vlan-id	VLAN name or number. The timeout period change applies only to entries that match the specified VLAN.
age *seconds*	Value for the timeout period, in seconds. You can specify a value from 0 through 1,000,000. If you change the timeout period to 0, aging is disabled.

Defaults

The aging timeout period is 300 seconds (5 minutes).

Mode

Enabled.

Example

The following command changes the aging timeout period to 600 seconds for entries that match VLAN *orange*:

```
RBT-8100# set fdb agingtime orange age 600
success: change accepted.
```

Related Commands

show fdb agingtime on page 5-16

set security l2-restrict

Restricts Layer 2 forwarding between clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, MSS allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN's default routers. Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified default routers.

Syntax

set security l2-restrict vlan *vlan-id* [**mode** {**enable** | **disable**}] [**permit-mac** *mac-addr* [*mac-addr*]]

Parameters

vlan-id	VLAN name or number.
mode {**enable** | **disable**}	Enables or disables restriction of Layer 2 forwarding.
permit-mac *mac-addr* [*mac-addr*]	MAC addresses to which clients are allowed to forward data at Layer 2. You can specify up to four addresses.

Defaults

Layer 2 restriction is disabled by default.

Mode

Enabled.

Usage

You can specify multiple addresses by listing them on the same command line or by entering multiple commands. To change a MAC address, use the **clear security l2-restrict** command to remove it, then use the **set security l2-restrict** command to add the correct address.

Restriction of client traffic does not begin until you enable the permitted MAC list. Use the **mode enable** option with this command.

Example

The following command restricts Layer 2 forwarding of client data in VLAN *abc_air* to the default routers with MAC address aa:bb:cc:dd:ee:ff and 11:22:33:44:55:66:

```
RBT-8100# set security l2-restrict vlan abc_air mode enable permit-mac
aa:bb:cc:dd:ee:ff 11:22:33:44:55:66
success: change accepted.
```

set vlan name

Creates a VLAN and assigns a number and name to it.

Syntax

set vlan *vlan-num* **name** *name*

Parameters

vlan-num	VLAN number. You can specify a number from 2 through 4093.
name *name*	String up to 16 alphabetic characters long.

Defaults

VLAN 1 is named *default* by default. No other VLANs have default names.

Mode

Enabled.

Usage

You must assign a name to a VLAN (other than the default VLAN) before you can add ports to the VLAN.

Enterasys Networks recommends that you do not use the name *default*. This name is already used for VLAN 1. Enterasys Networks also recommends that you do not rename the default VLAN.

You cannot use a number as the first character in the VLAN name. Enterasys Networks recommends that you do not use the same name with different capitalizations for VLANs. For example, do not configure two separate VLANs with the names *red* and *RED*.

VLAN names are case-sensitive for RADIUS authorization when a client roams to a RoamAbout switch. If the switch is not configured with the VLAN the client is on, but is configured with a VLAN that has the same spelling but different capitalization, authorization for the client fails. For example, if the client is on VLAN *red* but the RoamAbout switch to which the client roams has VLAN *RED* instead, RADIUS authorization fails.

Example

The following command assigns the name *marigold* to VLAN 3:

```
RBT-8100# set vlan 3 name marigold
success: change accepted.
```

Related Commands

set vlan port on page 5-12

set vlan port

Assigns one or more network ports to a VLAN. You also can add a virtual port to each network port by adding a tag value to the network port.

Syntax

set vlan *vlan-id* **port** *port-list* [**tag** *tag-value*]

Parameters

vlan-id	VLAN name or number.
port *port-list*	List of physical ports.
tag *tag-value*	Tag value that identifies a virtual port. You can specify a value from 1 through 4093.

Defaults

By default, no ports are members of any VLANs. A RoamAbout switch cannot forward traffic on the network until you configure VLANs and add network ports to the VLANs.

Mode

Enabled.

Usage

You can combine this command with the **set port name** command to assign the name and add the ports at the same time.

If you do not specify a tag value, the RoamAbout switch sends untagged frames for the VLAN. If you do specify a tag value, the switch sends tagged frames only for the VLAN.

If you do specify a tag value, Enterasys Networks recommends that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same but some other vendors' devices do.

Examples

The following command assigns the name *beige* to VLAN 11 and adds ports 1 through 3 to the VLAN:

```
RBT-8100# set vlan 11 name beige port 1-3
success: change accepted.
```

The following command adds port 16 to VLAN *beige* and assigns tag value 86 to the port:

```
RBT-8100# set vlan beige port 16 tag 86
success: change accepted.
```

Related Commands

- clear vlan on page 5-6
- set security l2-restrict on page 5-10
- show vlan config on page 5-24

set vlan tunnel-affinity

Changes a RoamAbout switch's preferability within a Mobility Domain for tunneling user traffic for a VLAN. When a user roams to a RoamAbout switch that is not a member of the user's VLAN, the switch can forward the user traffic by tunneling to another RoamAbout switch that is a member of the VLAN.

Syntax

`set vlan` *vlan-id* **`tunnel-affinity`** *num*

Parameters

vlan-id	VLAN name or number.
tunnel-affinity *num*	Preference of this switch for forwarding user traffic for the VLAN. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults

Each VLAN on a RoamAbout switch's network ports has an affinity value of 5 by default.

Mode

Enabled.

Usage

Increasing a switch's affinity value increases the switch's preferability for forwarding user traffic for the VLAN.

If more than one RoamAbout switch has the highest affinity value, MSS randomly selects one of the switches for the tunnel.

Example

The following command changes the VLAN affinity for VLAN *beige* to 10:

```
RBT-8100# set vlan beige tunnel-affinity 10
success: change accepted.
```

Related Commands

- show roaming vlan on page 5-20
- show vlan config on page 5-24

show fdb

Displays entries in the forwarding database.

Syntax

show fdb [*mac-addr-glob* [**vlan** *vlan-id*]]

show fdb {**perm** | **static** | **dynamic** | **system** | **all**} [**port** *port-list* | **vlan** *vlan-id*]

Parameters

mac-addr-glob	A single MAC address or set of MAC addresses. Specify a MAC address, or use the wildcard character (*) to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 1-4.)
vlan *vlan-id*	Name or number of a VLAN for which to display entries.
perm	Displays permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Displays static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
dynamic	Displays dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
system	Displays system entries. A system entry is added by MSS. For example, the authentication protocols can add entries for wired and wireless authentication users.
all	Displays all entries in the database, or all the entries that match a particular port or ports or a particular VLAN.
port *port-list*	Destination port(s) for which to display entries.

Defaults

None.

Mode

All.

Usage

To display the entire forwarding database, enter the **show fdb** command without options. To display only a portion of the database, use optional parameters to specify the types of entries you want to display.

Example

The following command displays all entries in the forwarding database:

```
RBT-8100# show fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ------------------ -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      aa:bb:cc:dd:ee:ff      *       3                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 3
```

The top line of the display identifies the characters to distinguish among the entry types.

The following command displays all entries that begin with the MAC address glob 00:

```
RBT-8100# show fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ------------------ -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 2
```

Table 5-1 describes the fields in the **show fdb** output.

Table 5-1 Output for show fdb

Output	What It Displays...
VLAN	VLAN number.
TAG	VLAN tag value. If the interface is untagged, the TAG field is blank.
Dest MAC/Route Des	MAC address of this forwarding entry's destination.
CoS	Type of entry. The entry types are explained in the first row of the command output. This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features.
Destination Ports	RoamAbout switch port associated with the entry. A switch sends traffic to the destination MAC address through this port.
Protocol Type	Layer 3 protocol address types that can be mapped to this entry.
Total Matching FDB Entries Displayed	Number of entries displayed by the command.

Related Commands

- clear fdb on page 5-2
- set fdb on page 5-8

show fdb agingtime

Displays the aging timeout period for forwarding database entries.

Syntax

show fdb agingtime [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the aging timeout period for each VLAN is displayed.

Defaults

None.

Mode

All.

Example

The following command displays the aging timeout period for all VLANs:

```
RBT-8100# show fdb agingtime
VLAN 2 aging time = 600 sec
VLAN 1 aging time = 300 sec
```

Because the forwarding database aging timeout period can be configured only on an individual VLAN basis, the command lists the aging timeout period for each VLAN separately.

Related Commands

set fdb agingtime on page 5-9

show fdb count

Lists the number of entries in the forwarding database.

Syntax

show fdb count {**perm** | **static** | **dynamic**} [**vlan** *vlan-id*]

Parameters

perm	Lists the number of permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Lists the number of static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
dynamic	Lists the number of dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
vlan *vlan-id*	VLAN name or number. Entries are listed for only the specified VLAN.

Defaults

None.

Mode

All.

Example

The following command lists the number of dynamic entries that the forwarding database contains:

```
RBT-8100# show fdb count dynamic
Total Matching Entries = 2
```

Related Commands

show fdb on page 5-14

show roaming station

Displays a list of the stations roaming to the RoamAbout switch through a VLAN tunnel.

Syntax

show roaming station [**vlan** *vlan-id*] [**peer** *ip-addr*]

Parameters

vlan *vlan-id*	Output is restricted to stations using this VLAN.
peer *ip-addr*	Output is restricted to stations tunnelling through this peer RoamAbout switch in the Mobility Domain.

Defaults

None.

Mode

Enabled.

Usage

The output displays roaming stations within the previous 1 second.

Example

To display all stations roaming to the RoamAbout switch, type the following command:

```
RBT-8100# show roaming station
User Name               Station IP Addr Old AP MAC        VLAN           State
----------------------- --------------- ----------------- -------------- ------
redsqa                  0.0.0.0         00:00:00:00:00:00 violet         Up
```

Table 5-2 describes the fields in the display.

Table 5-2 Output for show roaming station

Output	What It Displays...
User Name	Name of the user. This is the name used for authentication. The name resides in a RADIUS server database or the local user database on a RoamAbout switch.
Station IP Addr	IP address of the user device.
VLAN	Name of the VLAN to which the RADIUS server or RoamAbout switch local user database assigned the user.

Table 5-2 Output for show roaming station (continued)

Output	What It Displays...
State	State of the session: Setup—Station is attempting to roam to this RoamAbout switch. This switch has asked the RoamAbout switch from which the station is roaming for the station's session information and is waiting for a reply. Up—MSS has established a tunnel between the RoamAbout switches and the station has successfully roamed to this RoamAbout switch over the tunnel. Chck—This RoamAbout switch is in the process of accepting a reassociation request from the roaming peer RoamAbout switch for a station currently roaming to the peer switch. TChck—This RoamAbout switch is in the process of accepting a reassociation request from the roaming peer RoamAbout switch for a station currently roaming to this switch. WInd—This RoamAbout switch is waiting for network congestion to clear before sending the roaming indication to the roaming peer RoamAbout switch. WResp—This RoamAbout switch is waiting for network congestion to clear before sending the roaming response to the roaming peer RoamAbout switch.

Related Commands

show roaming vlan on page 5-20

show roaming vlan

Shows all VLANs in the Mobility Domain, the RoamAbout switches servicing the VLANs, and their tunnel affinity values configured on each switch for the VLANs.

Syntax

show roaming vlan

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following command shows the current roaming VLANs:

```
RBT-8100# show roaming vlan
VLAN             RBT              Affinity
---------------- ---------------- --------
vlan-cs          192.168.14.2            5
vlan-eng         192.168.14.4            5
vlan-fin         192.168.14.2            5
vlan-it          192.168.14.4            5
vlan-it          192.168.14.2            5
vlan-pm          192.168.14.2            5
vlan-sm          192.168.14.2            5
vlan-tp          192.168.14.4            5
vlan-tp          192.168.14.2            5
```

Table 5-3 describes the fields in the display.

Table 5-3 Output for show roaming vlan

Output	What It Displays...
VLAN	VLAN name.
RoamAbout switch	System IP address of the RoamAbout switch on which the VLAN is configured.
Affinity	Preference of this switch for forwarding user traffic for the VLAN. A higher number indicates a greater preference.

Related Commands

- show roaming station on page 5-18
- show vlan config on page 5-24

show security l2-restrict

Displays configuration information and statistics for Layer 2 forwarding restriction.

Syntax

show security l2-restrict [**vlan** *vlan-id* | **all**]

Parameters

vlan-id	VLAN name or number.
all	Displays information for all VLANs.

If you do not specify a VLAN name or **all**, information is displayed for all VLANs.

Mode

Enabled.

Defaults

None.

Example

The following command shows Layer 2 forwarding restriction information for all VLANs:

```
RBT-8100# show security l2-restrict
VLAN Name             En Drops      Permit MAC          Hits
---- ---------------- -- ---------- ------------------ ----------
   1 default          Y           0 00:0b:0e:02:53:3e         5947
                                    00:30:b6:3e:5c:a8            9
   2 vlan-2           Y           0 04:04:04:04:04:04          0
```

Table 5-4 describes the fields in the display.

Table 5-4 Output for show security l2-restrict

Field	Description
VLAN	VLAN number.
Name	VLAN name.
En	Enabled state of the feature for the VLAN: • Y—Enabled. Forwarding of Layer 2 traffic from clients is restricted to the MAC address(es) listed under Permit MAC. • N—Disabled. Layer 2 forwarding is not restricted.
Drops	Number of packets dropped because the destination MAC address was not one of the addresses listed under Permit MAC.
Permit MAC	MAC addresses to which clients in the VLAN are allowed to send traffic at Layer 2.

Table 5-4 Output for show security l2-restrict

Field	Description
Hits	Number of packets whose source MAC address was a client in this VLAN, and whose destination MAC address was one of those listed under Permit MAC.

show tunnel

Displays the tunnels from the RoamAbout switch where you type the command.

Syntax

show tunnel

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

To display all tunnels from a RoamAbout switch to other switches in the Mobility Domain, type the following command.

```
RBT-8100# show tunnel
VLAN            Local Address   Remote Address  State   Port  LVID  RVID
--------------- --------------- --------------- ------- ----- ----- -----
vlan-eng        192.168.14.2    192.168.14.4    DORMANT  1024  4096   130
```

Table 5-5 describes the fields in the display.

Table 5-5 Output for show tunnel

Output	What It Displays...
VLAN	VLAN name.
Local Address	IP address of the local end of the tunnel. This is the system IP address of the RoamAbout switch where you enter the command.
Remote Address	IP address of the remote end of the tunnel. This is the system IP address of another RoamAbout switch in the Mobility Domain.
State	Tunnel state: Up Dormant
Port	Tunnel port ID.
LVID	Local VLAN ID.
RVID	Remote VLAN ID.

Related Commands

show vlan config on page 5-24

show vlan config

Displays VLAN information.

Syntax

show vlan config [*vlan-id*]

Parameters

vlan-id	VLAN name or number. If you do not specify a VLAN, information for all VLANs is displayed.

Defaults

None.

Mode

All.

Example

The following command displays information for VLAN *burgundy*:

```
RBT-8100# show vlan config burgundy
                      Admin  VLAN  Tunl                          Port
VLAN Name             Status State Affin Port              Tag   State
---- ---------------- ------ ----- ----- ----------------- ----- -----
   2 burgundy         Up     Up        5
                                         2                  none Up
                                         3                  none Up
                                         4                  none Up
                                         6                  none Up
                                         11                 none Up
                                         t:10.10.40.4       none Up
```

Table 5-6 describes the fields in this display.

Table 5-6 Output for show vlan config

Output	What It Displays...
VLAN	VLAN number.
Name	VLAN name.
Admin Status	Administrative status of the VLAN: Down—The VLAN is disabled. Up—The VLAN is enabled.
VLAN State	Link status of the VLAN: Down—The VLAN is not connected. Up—The VLAN is connected.
Tunl Affin	Tunnel affinity value assigned to the VLAN.
Port	Member port of the VLAN. The port can be a physical port or a virtual port. Physical ports are 10/100 Ethernet or gigabit Ethernet ports on the switch, and are listed by port number. Virtual ports are tunnels to other switches in a Mobility Domain, and are listed as follows: t:*ip-addr*, where *ip-addr* is the system IP address of the RoamAbout switch at the other end of the tunnel. This field can include AP access ports and wired authentication ports, because MSS dynamically adds these ports to a VLAN when handling user traffic for the VLAN.
Tag	Tag value assigned to the port.
Port State	Link state of the port: Down—The port is not connected. Up—The port is connected.

Related Commands

- clear vlan on page 5-6
- set security l2-restrict on page 5-10
- set vlan port on page 5-12
- set vlan tunnel-affinity on page 5-13

6

QoS Commands

Use Quality of Service (QoS) commands to configure packet prioritization in MSS. Packet prioritization ensures that RoamAbout Switches and RoamAbout Access Points give preferential treatment to high-priority traffic such as voice and video.

(To override the prioritization for specific traffic, use access controls lists [ACLs] to set the Class of Service [CoS] for the packets. See Chapter 14, Security ACL Commands.)

This chapter presents QoS commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear qos	6-2
set qos cos-to-dscp-map	6-3
set qos dscp-to-cos-map	6-4
show qos	6-5
show qos dscp-table	6-6

clear qos

Resets switch mapping of Differentiated Services Code Point (DSCP) to internal QoS values.

The switch's internal QoS map ensures that prioritized traffic remains prioritized while transiting through the RoamAbout Switch. An RoamAbout Switch uses the QoS map to do the following:

- Classify inbound packets by mapping their DSCP values to one of eight internal QoS values
- Classify outbound packets by marking their DSCP values based on the switch's internal QoS values

Syntax

clear qos
[**cos-to-dscp-map** [*from-qos*] | **dscp-to-cos-map** [*from-dscp*]]

Parameters

cos-to-dscp-map [*from-qos*]	Resets the mapping between the specified internal QoS value and the DSCP values with which MSS marks outbound packets. QoS values are from 0 to 7.
dscp-to-cos-map [*from-dscp*]	Resets the mapping between the specified range of DSCP values and internal QoS value with which MSS classifies inbound packets.

Defaults

None.

Mode

Enabled.

Usage

To reset all mappings to their default values, use the **clear qos** command without the optional parameters.

Examples

The following command resets all QoS mappings:

```
RBT-8100# clear qos
success: change accepted.
```

The following command resets the mapping used to classify packets with DSCP value 44:

```
RBT-8100# clear qos dscp-to-qos-map 44
success: change accepted.
```

set qos cos-to-dscp-map

Changes the value to which MSS maps an internal QoS value when marking outbound packets.

Syntax

set qos cos-to-dscp-map *level* **dscp** *dscp-value*

Parameters

level	Internal CoS value. You can specify a number from 0 to 7.
dscp *dscp-value*	DSCP value. You can specify the value as a decimal number. Valid values are 0 to 63.

Defaults

The defaults are listed by the **show qos** command.

Mode

Enabled.

Example

The following command maps internal CoS value 5 to DSCP value 50:

```
RBT-8100# set qos cos-to-dscp-map 5 dscp 50
```

Caution: cos 5 is marked with dscp 50 which will be classified as cos 6.

If the change results in a change to CoS, MSS displays a warning message indicating the change. In this example, packets that receive CoS 5 upon ingress will be marked with a DSCP value equivalent to CoS 6 upon egress.

Related Commands

- set qos dscp-to-cos-map on page 6-4
- show qos on page 6-5

set qos dscp-to-cos-map

Changes the internal QoS value to which MSS maps a packet's DSCP value when classifying inbound packets.

Syntax

set qos dscp-to-cos-map *dscp-range* **cos** *level*

Parameters

dscp-range	DSCP range. You can specify the values as decimal numbers. Valid decimal values are 0 to 63. To specify a range, use the following format: 40-56. Specify the lower number first.
cos *level*	Internal QoS value. You can specify a number from 0 to 7.

Defaults

The defaults are listed by the **show qos** command.

Mode

Enabled.

Example

The following command maps DSCP values 40-56 to internal CoS value 6:

```
RBT-8100# set qos dscp-to-cos-map 40-56 cos 6
warning: cos 5 is marked with dscp 63 which will be classified as cos 7
warning: cos 7 is marked with dscp 56 which will be classified as cos 6
```

As shown in this example, if the change results in a change to CoS, MSS displays a warning message indicating the change.

Related Commands

- set qos cos-to-dscp-map on page 6-3
- show qos on page 6-5

show qos

Displays the switch's QoS settings.

Syntax

show qos [**default**]

Parameters

default	Displays the default mappings.

Defaults

None.

Mode

Enabled.

Example

The following command displays the default QoS settings:

```
RBT-8100# show qos default

Ingress QoS Classification Map (dscp-to-cos)

Ingress DSCP       CoS Level
================================================================================
       00-09       0    0    0    0    0      0    0    0    1    1
       10-19       1    1    1    1    1      1    2    2    2    2
       20-29       2    2    2    2    3      3    3    3    3    3
       30-39       3    3    4    4    4      4    4    4    4    4
       40-49       5    5    5    5    5      5    5    5    6    6
       50-59       6    6    6    6    6      6    7    7    7    7
       60-63       7    7    7    7

Egress QoS Marking Map (cos-to-dscp)

CoS Level              0      1      2      3      4      5      6      7
================================================================================
Egress DSCP            0      8     16     24     32     40     48     56
Egress ToS byte      0x00   0x20   0x40   0x60   0x80   0xA0   0xC0   0xE0
```

Related Commands

show qos dscp-table on page 6-6

show qos dscp-table

Displays a table that maps Differentiated Services Code Point (DSCP) values to their equivalent combinations of IP precedence values and IP ToS values.

Syntax

show qos dscp-table

Parameters

None.

Mode

Enabled.

Usage

Introduced in MSS v4.0 as the **show security acl dscp** command and renamed in v4.1.

Example

The following command displays the table:

```
RBT-8100# show qos dscp-table

DSCP           TOS            precedence    tos
dec  hex       dec  hex
-----------------------------------------------
  0  0x00        0  0x00               0      0
  1  0x01        4  0x04               0      2
  2  0x02        8  0x08               0      4
...
 63  0x3f      252  0xfc               7     14
```

Related Commands

show qos on page 6-5

7

IP Services Commands

Use IP services commands to configure and manage IP interfaces, management services, the Domain Name Service (DNS), Network Time Protocol (NTP), and aliases, and to ping a host or trace a route. This chapter presents IP services commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear interface	7-4
clear ip alias	7-5
clear ip dns domain	7-6
clear ip dns server	7-7
clear ip route	7-8
clear ip telnet	7-9
clear ntp server	7-10
clear ntp update-interval	7-11
clear snmp community	7-12
clear snmp notify target	7-13
clear snmp notify profile	7-14
clear snmp trap receiver	7-15
clear snmp usm	7-16
clear summertime	7-17
clear system ip-address	7-18
clear timezone	7-19
ping	7-20
set arp	7-22
set arp agingtime	7-23
set interface	7-24
set interface dhcp-client	7-25
set interface dhcp-server	7-26
set interface status	7-28

For information about...	Refer to page...
set ip alias	7-29
set ip dns	7-30
set ip dns domain	7-31
set ip dns server	7-32
set ip https server	7-33
set ip route	7-34
set ip https server	7-33
set ip route	7-34
set ip snmp server	7-36
set ip ssh	7-37
set ip ssh server	7-38
set ip telnet	7-39
set ip telnet server	7-40
set ntp	7-41
set ntp server	7-42
set ntp update-interval	7-43
set snmp community	7-44
set snmp notify target	7-46
set snmp profile	7-51
set snmp protocol	7-56
set snmp security	7-57
set snmp trap	7-58
set snmp trap receiver	7-59
set snmp usm	7-60
set summertime	7-63
set system ip-address	7-65
set timedate	7-66
set timezone	7-67
show arp	7-68
show dhcp-client	7-70
show dhcp-server	7-72
show interface	7-75
show ip alias	7-77
show ip dns	7-78

For information about...	Refer to page...
show ip https	7-80
show ip route	7-82
show ip telnet	7-84
show ntp	7-85
show snmp configuration	7-87
show snmp community	7-89
show snmp counters	7-90
show snmp notify profile	7-91
show snmp notify target	7-92
show snmp status	7-93
show snmp usm	7-94
show summertime	7-95
show timedate	7-96
show timezone	7-97
telnet	7-98
traceroute	7-100

clear interface

Removes an IP interface.

Syntax

clear interface *vlan-id* **ip**

Parameters

vlan-id	VLAN name or number.

Defaults

None.

Mode

Enabled.

Usage

If the interface you want to remove is configured as the system IP address, removing the address can interfere with system tasks that use the system IP address, including the following:

- Mobility domain operations
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Example

The following command removes the IP interface configured on VLAN *mauve*:

```
RBT-8100# clear interface mauve ip
success: cleared ip on vlan mauve
```

Related Commands

- set interface on page 7-24
- set interface status on page 7-28
- show interface on page 7-75

clear ip alias

Removes an alias, which is a string that represents an IP address.

Syntax

clear ip alias *name*

Parameters

name	Alias name.

Defaults

None.

Mode

Enabled.

Example

The following command removes the alias *server1*:

```
RBT-8100# clear ip alias server1
success: change accepted.
```

Related Commands

- set ip alias on page 7-29
- show ip alias on page 7-77

clear ip dns domain

Removes the default DNS domain name.

Syntax

clear ip dns domain

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following command removes the default DNS domain name from a RoamAbout switch:

```
RBT-8100# clear ip dns domain
Default DNS domain name cleared.
```

Related Commands

- clear ip dns server on page 7-7
- set ip dns on page 7-30
- set ip dns domain on page 7-31
- set ip dns server on page 7-32
- show ip dns on page 7-78

clear ip dns server

Removes a DNS server from a RoamAbout switch configuration.

Syntax

clear ip dns server *ip-addr*

Parameters

ip-addr	IP address of a DNS server.

Defaults

None.

Mode

Enabled.

Example

The following command removes DNS server 10.10.10.69 from a RoamAbout switch's configuration:

```
RBT-8100# clear ip dns server 10.10.10.69
success: change accepted.
```

Related Commands

- clear ip dns domain on page 7-6
- set ip dns on page 7-30
- set ip dns domain on page 7-31
- set ip dns server on page 7-32
- show ip dns on page 7-78

clear ip route

Removes a route from the IP route table.

Syntax

clear ip route {**default** | *ip-addr mask* | *ip-addr/mask-length*} *default-router*

Parameters

default	Default route. **Note: default** is an alias for IP address 0.0.0.0/0.
ip-addr mask	IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
ip-addr/mask-length	IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).
default-router	IP address, DNS hostname, or alias of the next-hop router.

Defaults

None.

Mode

Enabled.

Example

The following command removes the route to destination 10.10.10.68/24 through router 10.10.10.1:

```
RBT-8100# clear ip route 10.10.10.68/24 10.10.10.1
success: change accepted.
```

Related Commands

- set ip route on page 7-34
- show ip route on page 7-82

clear ip telnet

Resets the Telnet server's TCP port number to its default value. A RoamAbout switch listens for Telnet management traffic on the Telnet server port.

Syntax

```
clear ip telnet
```

Parameters

None.

Defaults

The default Telnet port number is 23.

Mode

Enabled.

Example

The following command resets the TCP port number for Telnet management traffic to its default:

```
RBT-8100# clear ip telnet
success: change accepted.
```

Related Commands

- set ip https server on page 7-33
- set ip telnet on page 7-39
- set ip telnet server on page 7-40
- show ip https on page 7-80
- show ip telnet on page 7-84

clear ntp server

Removes an NTP server from a RoamAbout switch configuration.

Syntax

clear ntp server {*ip-addr* | **all**}

Parameters

ip-addr	IP address of the server to remove, in dotted decimal notation.
all	Removes all NTP servers from the configuration.

Defaults

None.

Mode

Enabled.

Example

The following command removes NTP server 192.168.40.240 from a RoamAbout switch configuration:

```
RBT-8100# clear ntp server 192.168.40.240
success: change accepted.
```

Related Commands

- clear ntp update-interval on page 7-11
- set ntp on page 7-41
- set ntp server on page 7-42
- set ntp update-interval on page 7-43
- show ntp on page 7-85

clear ntp update-interval

Resets the NTP update interval to the default value.

Syntax

```
clear ntp update-interval
```

Parameters

None.

Defaults

The default NTP update interval is 64 seconds.

Mode

Enabled.

Example

To reset the NTP interval to the default value, type the following command:

```
RBT-8100# clear ntp update-interval
success: change accepted.
```

Related Commands

- clear ntp server on page 7-10
- set ntp on page 7-41
- set ntp server on page 7-42
- set ntp update-interval on page 7-43
- show ntp on page 7-85

clear snmp community

Clears an SNMP community string.

Syntax

clear snmp community name *comm-string*

Parameters

comm-string	Name of the SNMP community you want to clear.

Defaults

None.

Mode

Enabled.

Example

The following command clears community string *setswitch2*:

```
RBT-8100# clear snmp community name setswitch2
success: change accepted.
```

Related Commands

- set snmp community on page 7-44
- show snmp community on page 7-89

clear snmp notify target

Clears an SNMP notification target.

Syntax

clear snmp notify target *target-num*

Parameters

target-num	ID of the target.

Defaults

None.

Mode

Enabled.

The following command clears notification target 3:

```
RBT-8100# clear snmp notify target 3
success: change accepted.
```

Related Commands

- set snmp notify target on page 7-46
- show snmp notify target on page 7-92

clear snmp notify profile

Clears an SNMP notification profile.

Syntax

clear snmp notify profile *profile-name*

Parameters

profile-name	Name of the notification profile you are clearing.

Defaults

None.

Mode

Enabled.

Example

The following command clears notification profile *snmpprof_rfdetect*:

```
RBT-8100# clear snmp notify profile snmpprof_rfdetect
success: change accepted.
```

Related Commands

- set snmp profile on page 7-51
- show snmp notify profile on page 7-91

clear snmp trap receiver

This command is deprecated in MSS Version 4.0. To clear an SNMP notification target (also called *trap receiver*), see clear snmp notify target on page 7-13.

Syntax

clear snmp trap receiver *ip-addr*

Parameters

ip-addr	IP address of the trap receiver, in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Example

To delete the trap receiver at IP address 192.168.0.1, type the following command:

```
RBT-8100# clear snmp trap receiver 192.168.0.1
success: change accepted.
```

Related Commands

- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp trap on page 7-58
- set snmp trap receiver on page 7-59

clear snmp usm

Clears an SNMPv3 user.

Syntax

clear snmp usm *usm-username*

Parameters

usm-username	Name of the SNMPv3 user you want to clear.

Defaults

None.

Mode

Enabled.

Example

The following command clears SNMPv3 user *snmpmgr1*:

```
RBT-8100# clear snmp usm snmpmgr1
success: change accepted.
```

Related Commands

- set snmp usm on page 7-60
- show snmp usm on page 7-94

clear summertime

Clears the summertime setting from a RoamAbout switch.

Syntax

```
clear summertime
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

To clear the summertime setting from a RoamAbout switch, type the following command:

```
RBT-8100# clear summertime
success: change accepted.
```

Related Commands

- clear timezone on page 7-19
- set summertime on page 7-63
- set timedate on page 7-66
- set timezone on page 7-67
- show summertime on page 7-95
- show timedate on page 7-96
- show timezone on page 7-97

clear system ip-address

Clears the system IP address.

Caution: Clearing the system IP address disrupts the system tasks that use the address.

Syntax

```
clear system ip-address
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Usage

Clearing the system IP address can interfere with system tasks that use the system IP address, including the following:

- Mobility Domain operations
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Example

To clear the system IP address, type the following command:

```
RBT-8100# clear system ip-address
success: change accepted.
```

Related Commands

- set system ip-address on page 7-65
- show system on page 3-26

clear timezone

Clears the time offset for the RoamAbout switch's real-time clock from Coordinated Universal Time (UTC). UTC is also know as Greenwich Mean Time (GMT).

Syntax

```
clear timezone
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

To return the RoamAbout switch's real-time clock to UTC, type the following command:

```
RBT-8100# clear timezone
success: change accepted.
```

Related Commands

- clear summertime on page 7-17
- set summertime on page 7-63
- set timedate on page 7-66
- set timezone on page 7-67
- show summertime on page 7-95
- show timedate on page 7-96
- show timezone on page 7-97

ping

Tests IP connectivity between a RoamAbout switch and another device. MSS sends an Internet Control Message Protocol (ICMP) echo packet to the specified device and listens for a reply packet.

Syntax

```
ping host [count num-packets] [dnf] [flood] [interval time] [size size]
[source-ip ip-addr | vlan-name]
```

Parameters

host	IP address, MAC address, hostname, alias, or user to ping.
count *num-packets*	Number of ping packets to send. You can specify from 0 through 2,147,483,647. If you enter 0, MSS pings continuously until you interrupt the command.
dnf	Enables the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented.
flood	Sends new ping packets as quickly as replies are received, or 100 times per second, whichever is greater. **Note:** Use the **flood** option sparingly. This option creates a lot of traffic and can affect other traffic on the network.
interval *time*	Time interval between ping packets, in milliseconds. You can specify from 100 through 10,000.
size *size*	Packet size, in bytes. You can specify from 56 through 65,507. **Note:** Because the switch adds header information, the ICMP packet size is 8 bytes larger than the size you specify.
source-ip *ip-addr*	IP address, in dotted decimal notation, to use as the source IP address in the ping packets.
source-ip *vlan-name*	VLAN name to use as the ping source. MSS uses the IP address configured on the VLAN as the source IP address in the ping packets.

Defaults

- **count**—5.
- **dnf**—Disabled.
- **interval**—100 (one tenth of a second)
- **size**—56.

Mode

Enabled.

Usage

To stop a **ping** command that is in progress, press Ctrl+C.

A RoamAbout switch cannot ping itself. MSS does not support this.

Example

The following command pings a device that has IP address 10.1.1.1:

```
RBT-8100# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss
```

Related Commands

traceroute on page 7-100

set arp

Adds an ARP entry to the ARP table.

Syntax

set arp {**permanent** | **static** | **dynamic**} *ip-addr mac-addr*

Parameters

permanent	Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
static	Adds a static entry. A static entry does not age out, but the entry does not remain in the database after a reboot, reset, or power cycle.
dynamic	Adds a dynamic entry. A dynamic entry is automatically removed if the entry ages out, or after a reboot, reset, or power cycle.
ip-addr	IP address of the entry, in dotted decimal notation.
mac-addr	MAC address to map to the IP address. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).

Defaults

None.

Mode

Enabled.

Example

The following command adds a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff:

```
RBT-8100# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

Related Commands

- set arp agingtime on page 7-23
- show arp on page 7-68

set arp agingtime

Changes the aging timeout for dynamic ARP entries.

Syntax

set arp agingtime *seconds*

Parameters

seconds	Number of seconds an entry can remain unused before MSS removes the entry. You can specify from 0 through 1,000,000. To disable aging, specify 0.

Defaults

The default aging timeout is 1200 seconds.

Mode

Enabled.

Usage

Aging applies only to dynamic entries.

To reset the ARP aging timeout to its default value, use the **set arp agingtime 1200** command.

Example

The following command changes the ARP aging timeout to 1800 seconds:

```
RBT-8100# set arp agingtime 1800
success: set arp aging time to 1800 seconds
```

The following command disables ARP aging:

```
RBT-8100# set arp agingtime 0
success: set arp aging time to 0 seconds
```

Related Commands

- set arp on page 7-22
- show arp on page 7-68

set interface

Configures an IP interface on a VLAN.

Syntax

set interface *vlan-id* **ip** {*ip-addr mask* | *ip-addr/mask-length*}

Parameters

vlan-id	VLAN name or number.
ip-addr mask	IP address and subnet mask in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
ip-addr/mask-length	IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

Defaults

None.

Mode

Enabled.

Usage

You can assign one IP interface to each VLAN.

If an interface is already configured on the VLAN you specify, this command replaces the interface. If you replace an interface that is in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- Mobility domain operations
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

The following command configures IP interface 10.10.10.10/24 on VLAN *default*:

```
RBT-8100# set interface default ip 10.10.10.10/24
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN *mauve*:

```
RBT-8100# set interface mauve ip 10.10.20.10 255.255.255.0
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```

Related Commands

- clear interface on page 7-4
- set interface status on page 7-28
- show interface on page 7-75

set interface dhcp-client

Configures the DHCP client on a VLAN, to allow the VLAN to obtain its IP interface from a DHCP server.

Syntax

```
set interface vlan-id ip dhcp-client {enable | disable}
```

Parameters

vlan-id	VLAN name or number.
enable	Enables the DHCP client on the VLAN.
disable	Disables the DHCP client on the VLAN.

Defaults

The DHCP client is disabled by default on all switch models.

Mode

Enabled.

Usage

You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

MSS also has a configurable DHCP server. (See set interface dhcp-server on page 7-26.) You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

Example

The following command enables the DHCP client on VLAN *corpvlan*:

```
RBT-8100# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

Related Commands

- clear interface on page 7-4
- show dhcp-client on page 7-70
- show interface on page 7-75

set interface dhcp-server

Configures the MSS DHCP server.

Note: Use of the MSS DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. Enterasys Networks recommends that you do not use the MSS DHCP server to allocate client addresses in a production network.

Syntax

set interface *vlan-id* **ip dhcp-server** [**enable** | **disable**] [**start** *ip-addr1* **stop** *ip-addr2*] [**dns-domain** *domain-name*] [**primary-dns** *ip-addr* [**secondary-dns** *ip-addr*]] [**default-router** *ip-addr*]

Parameters

vlan-id	VLAN name or number.
enable	Enables the DHCP server.
disable	Disables the DHCP server.
start *ip-addr1*	Specifies the beginning address of the address range (also called the address *pool*).
stop *ip-addr2*	Specifies the ending address of the address range.
dns-domain *domain-name*	Name of the DHCP client's default DNS domain.
primary-dns *ip-addr* [**secondary-dns** *ip-addr*]	IP addresses of the DHCP client's DNS servers.
default-router *ip-addr*	IP address of the DHCP client's default router.

Defaults

The DHCP server is disabled by default.

Mode

Enabled.

Usage

By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

Specification of the DNS domain name, DNS servers, and default router are optional. If you omit one or more of these options, the MSS DHCP server uses oath values configured elsewhere on the switch:

- DNS domain name—If this option is not set with the **set interface dhcp-server** command's **dns-domain** option, the MSS DHCP server uses the value set by the **set ip dns domain** command.
- DNS servers—If these options are not set with the **set interface dhcp-server** command's **primary-dns** and **secondary-dns** options, the MSS DHCP server uses the values set by the **set ip dns server** command.

- Default router—If this option is not set with the **set interface dhcp-server** command's **default-router** option, the MSS DHCP server can use the value set by the **set ip route** command. A default route configured by **set ip route** can be used if the route is in the DHCP client's subnet. Otherwise, the MSS DHCP server does not specify a router address.

Example

The following command enables the DHCP server on VLAN *red-vlan* to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
RBT-8100# set interface red-vlan ip dhcp-server enable start 192.168.1.5 stop
192.168.1.25
success: change accepted.
```

Related Commands

- set ip dns domain on page 7-31
- set ip dns server on page 7-32

set interface status

Administratively disables or reenables an IP interface.

Syntax

set interface *vlan-id* **status** {**up** | **down**}

Parameters

vlan-id	VLAN name or number.
up	Enables the interface.
down	Disables the interface.

Defaults

IP interfaces are enabled by default.

Mode

Enabled.

Example

The following command disables the IP interface on VLAN *mauve*:

```
RBT-8100# set interface mauve status down
success: set interface mauve to down
```

Related Commands

- clear interface on page 7-4
- set interface on page 7-24
- show interface on page 7-75

set ip alias

Configures an alias, which maps a name to an IP address. You can use aliases as shortcuts in CLI commands.

Syntax

set ip alias *name ip-addr*

Parameters

name	String of up to 32 alphanumeric characters, with no spaces.
ip-addr	IP address in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Example

The following command configures the alias *HR1* for IP address 192.168.1.2:

```
RBT-8100# set ip alias HR1 192.168.1.2
success: change accepted.
```

Related Commands

- clear ip alias on page 7-5
- show ip alias on page 7-77

set ip dns

Enables or disables DNS on a RoamAbout switch.

Syntax

```
set ip dns {enable | disable}
```

Parameters

enable	Enables DNS.
disable	Disables DNS.

Defaults

DNS is disabled by default.

Mode

Enabled.

Example

The following command enables DNS on a RoamAbout switch:

```
RBT-8100# set ip dns enable
Start DNS Client
```

Related Commands

- clear ip dns domain on page 7-6
- clear ip dns server on page 7-7
- set ip dns domain on page 7-31
- set ip dns server on page 7-32
- show ip dns on page 7-78

set ip dns domain

Configures a default domain name for DNS queries. The RoamAbout switch appends the default domain name to domain names or hostnames you enter in commands.

Syntax

set ip dns domain *name*

Parameters

name	Domain name of between 1 and 64 alphanumeric characters with no spaces (for example, example.org).

Defaults

None.

Mode

Enabled.

Usage

To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is *example.com*, enter **chris.** if the fully qualified hostname is *chris* and not *chris.example.com*.

Aliases take precedence over DNS. When you enter a hostname, MSS checks for an alias with that name first, before using DNS to resolve the name.

Example

The following command configures the default domain name *example.com*:

```
RBT-8100# set ip dns domain example.com
Domain name changed
```

Related Commands

- clear ip dns domain on page 7-6
- clear ip dns server on page 7-7
- set ip dns on page 7-30
- set ip dns server on page 7-32
- show ip dns on page 7-78

set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

Syntax

set ip dns server *ip-addr* {**primary** | **secondary**}

Parameters

ip-addr	IP address of a DNS server, in dotted decimal or CIDR notation.
primary	Makes the server the primary server, which MSS always consults first for resolving DNS queries.
secondary	Makes the server a secondary server. MSS consults a secondary server only if the primary server does not reply.

Defaults

None.

Mode

Enabled.

Usage

You can configure a RoamAbout switch to use one primary DNS server and up to five secondary DNS servers.

Example

The following commands configure a RoamAbout switch to use a primary DNS server and two secondary DNS servers:

```
RBT-8100# set ip dns server 10.10.10.50/24 primary
success: change accepted.
RBT-8100# set ip dns server 10.10.20.69/24 secondary
success: change accepted.
RBT-8100# set ip dns server 10.10.30.69/24 secondary
success: change accepted.
```

Related Commands

- clear ip dns domain on page 7-6
- clear ip dns server on page 7-7
- set ip dns on page 7-30
- set ip dns domain on page 7-31
- show ip dns on page 7-78

set ip https server

Enables the HTTPS server on a RoamAbout switch. The HTTPS server is required for WebView access to the switch.

Caution: If you disable the HTTPS server, Web View access to the switch is disabled.

Syntax

set ip https server {**enable** | **disable**}

Parameters

enable	Enables the HTTPS server.
disable	Disables the HTTPS server.

Defaults

The HTTPS server is disabled by default.

Mode

Enabled.

Example

The following command enables the HTTPS server on a RoamAbout switch:

```
RBT-8100# set ip https server enable
success: change accepted.
```

Related Commands

- clear ip telnet on page 7-9
- set ip telnet on page 7-39
- set ip telnet server on page 7-40
- show ip https on page 7-80
- show ip telnet on page 7-84

set ip route

Adds a static route to the IP route table.

Syntax

set ip route {**default** | *ip-addr mask* | *ip-addr/mask-length*} *default-router metric*

Parameters

default	Default route. A RoamAbout switch uses the default route if an explicit route is not available for the destination. **Note: default** is an alias for IP address 0.0.0.0/0.
ip-addr mask	IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
ip-addr/mask-length	IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).
default-router	IP address, DNS hostname, or alias of the next-hop router.
metric	Cost for using the route. You can specify a value from 0 through 2,147,483,647. Lower-cost routes are preferred over higher-cost routes.

Defaults

None.

Mode

Enabled.

Usage

MSS can use a static route only if a direct route in the route table resolves the static route. MSS adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is up. If one of these added routes can resolve the static route, MSS can use the static route.

Before you add a static route, use the **show interface** command to verify that the switch has an IP interface in the same subnet as the route's next-hop router. If not, the VLAN:Interface field of the **show ip route** command output shows that the route is down.

You can configure a maximum of 4 routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique router address. When the route table contains multiple default or explicit routes to the same destination, MSS uses the route with the lowest cost. If two or more routes to the same destination have the lowest cost, MSS selects the first route in the route table.

When you add multiple routes to the same destination, MSS groups the routes and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, MSS places the new route at the top of the group of routes with the same cost.

Example

The following command adds a default route that uses default router 10.5.4.1 and gives the route a cost of 1:

```
RBT-8100# set ip route default 10.5.4.1 1
success: change accepted.
```

The following commands add two default routes, and configure MSS to always use the route through 10.2.4.69 when the RoamAbout switch interface to that default router is up:

```
RBT-8100# set ip route default 10.2.4.69 1
success: change accepted.
RBT-8100# set ip route default 10.2.4.17 2
success: change accepted.
```

The following command adds an explicit route from a RoamAbout switch to any host on the 192.168.4.*x* subnet through the local router 10.5.4.2, and gives the route a cost of 1:

```
RBT-8100# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

The following command adds another explicit route, using CIDR notation to specify the subnet mask:

```
RBT-8100# set ip route 192.168.5.0/24 10.5.5.2 1
success: change accepted.
```

Related Commands

- clear ip route on page 7-8
- show interface on page 7-75
- show ip route on page 7-82

set ip snmp server

Enables or disables the SNMP service on the RoamAbout switch.

Syntax

```
set ip snmp server {enable | disable}
```

Parameters

enable	Enables the SNMP service.
disable	Disables the SNMP service.

Defaults

The SNMP service is disabled by default.

Mode

Enabled.

Example

The following command enables the SNMP server on a RoamAbout switch:

```
RBT-8100# set ip snmp server enable
success: change accepted.
```

Related Commands

- clear snmp trap receiver on page 7-15
- set port trap on page 4-25
- set snmp community on page 7-44
- set snmp trap on page 7-58
- set snmp trap receiver on page 7-59
- show snmp configuration on page 7-87

set ip ssh

Changes the TCP port number on which a RoamAbout switch listens for Secure Shell (SSH) management traffic.

Caution: If you change the SSH port number from an SSH session, MSS immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.

Syntax

set ip ssh port *port-num*

Parameters

port-num	TCP port number.

Defaults

The default SSH port number is 22.

Mode

Enabled.

Example

The following command changes the SSH port number on a RoamAbout switch to 6000:

```
RBT-8100# set ip ssh port 6000
success: change accepted.
```

Related Commands

- set ip ssh server on page 7-38
- set ip ssh server on page 7-38
- set ip ssh server on page 7-38

set ip ssh server

Disables or reenables the SSH server on a RoamAbout switch.

Caution: If you disable the SSH server, SSH access to the RoamAbout switch is also disabled.

Syntax

```
set ip ssh server {enable | disable}
```

Parameters

enable	Enables the SSH server.
disable	Disables the SSH server.

Defaults

The SSH server is enabled by default.

Mode

Enabled.

Usage

SSH requires an SSH authentication key. You can generate one or allow MSS to generate one. The first time an SSH client attempts to access the SSH server on a RoamAbout Switch, the switch automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

The maximum number of SSH sessions supported on a RoamAbout switch is eight. If Telnet is also enabled, the switch can have up to eight Telnet or SSH sessions, in any combination, and one Console session.

Related Commands

- crypto generate key on page 15-6
- set ip ssh on page 7-37
- set ip ssh server on page 7-38
- set ip ssh server on page 7-38

set ip telnet

Changes the TCP port number on which a RoamAbout switch listens for Telnet management traffic.

Caution: If you change the Telnet port number from a Telnet session, MSS immediately ends the session. To open a new management session, you must Telnet to the switch with the new Telnet port number.

Syntax

set ip telnet *port-num*

Parameters

port-num	TCP port number.

Defaults

The default Telnet port number is 23.

Mode

Enabled.

Example

The following command changes the Telnet port number on a RoamAbout switch to 5000:

```
RBT-8100# set ip telnet 5000
success: change accepted.
```

Related Commands

- clear ip telnet on page 7-9
- set ip https server on page 7-33
- set ip telnet server on page 7-40
- show ip https on page 7-80
- show ip telnet on page 7-84

set ip telnet server

Enables the Telnet server on a RoamAbout switch.

Caution: If you disable the Telnet server, Telnet access to the RoamAbout switch is also disabled.

Syntax

```
set ip telnet server {enable | disable}
```

Parameters

enable	Enables the Telnet server.
disable	Disables the Telnet server.

Defaults

The Telnet server is disabled by default.

Mode

Enabled.

Usage

The maximum number of Telnet sessions supported on a RoamAbout switch is eight. If SSH is also enabled, the switch can have up to eight Telnet or SSH sessions, in any combination, and one console session.

Example

The following command enables the Telnet server on a RoamAbout switch:

```
RBT-8100# set ip telnet server enable
success: change accepted.
```

Related Commands

- clear ip telnet on page 7-9
- set ip https server on page 7-33
- set ip telnet on page 7-39
- show ip https on page 7-80
- show ip telnet on page 7-84

set ntp

Enables or disables the NTP client on a RoamAbout switch.

Syntax

```
set ntp {enable | disable}
```

Parameters

enable	Enables the NTP client.
disable	Disables the NTP client.

Defaults

The NTP client is disabled by default.

Mode

Enabled.

Usage

If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the RoamAbout switch time can take many NTP update intervals. Enterasys Networks recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

Example

The following command enables the NTP client:

```
RBT-8100# set ntp enable
success: NTP Client enabled
```

Related Commands

- clear ntp server on page 7-10
- clear ntp update-interval on page 7-11
- set ntp server on page 7-42
- set ntp update-interval on page 7-43
- show ntp on page 7-85

set ntp server

Configures a RoamAbout switch to use an NTP server.

Syntax

set ntp server *ip-addr*

Parameters

ip-addr	IP address of the NTP server, in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Usage

You can configure up to three NTP servers. MSS queries all the servers and selects the best response based on the method described in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

To use NTP, you also must enable the NTP client with the **set ntp** command.

Example

The following command configures a RoamAbout switch to use NTP server 192.168.1.5:

```
RBT-8100# set ntp server 192.168.1.5
```

Related Commands

- clear ntp server on page 7-10
- clear ntp update-interval on page 7-11
- set ntp on page 7-41
- set ntp update-interval on page 7-43
- show ntp on page 7-85

set ntp update-interval

Changes how often MSS sends queries to the NTP servers for updates.

Syntax

set ntp update-interval *seconds*

Parameters

seconds	Number of seconds between queries. You can specify from 16 through 1024 seconds.

Defaults

The default NTP update interval is 64 seconds.

Mode

Enabled.

Example

The following command changes the NTP update interval to 128 seconds:

```
RBT-8100# set ntp update-interval 128
success: change accepted.
```

Related Commands

- clear ntp server on page 7-10
- clear ntp update-interval on page 7-11
- set ntp on page 7-41
- set ntp server on page 7-42
- show ntp on page 7-85

set snmp community

Configures a community string for SNMPv1 or SNMPv2c.

Note: For SNMPv3, use the **set snmp usm** command to configure an SNMPv3 user. SNMPv3 does not use community strings.

Syntax

set snmp community name *comm-string* **access** {**read-only** | **read-notify** | **notify-only** | **read-write** | **notify-read-write**}

Parameters

comm-string	Name of the SNMP community. Specify between 1 and 32 alphanumeric characters, with no spaces.
read-only	Allows an SNMP management application using the string to get (read) object values on the switch but not to set (write) them.
read-notify	Allows an SNMP management application using the string to get object values on the switch but not to set them. The switch can use the string to send notifications.
notify-only	Allows the switch to use the string to send notifications.
read-write	Allows an SNMP management application using the string to get and set object values on the switch.
notify-read-write	Allows an SNMP management application using the string to get and set object values on the switch. The switch also can use the string to send notifications.

Defaults

None.

Mode

Enabled.

Usage

SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. Enterasys Networks recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings *public* and *private*.

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt SNMP data.

Examples

The following command configures the read-write community *good_community*:

```
RBT-8100# set snmp community read-write good_community
success: change accepted.
```

The following command configures community string *switchmgr1* with access level **notify-read-write**:

```
RBT-8100# set snmp community name switchmgr1 notify-read-write
success: change accepted.
```

Related Commands

- clear snmp community on page 7-12
- set ip snmp server on page 7-36
- set snmp notify target on page 7-46
- set snmp profile on page 7-51
- set snmp protocol on page 7-56
- set snmp security on page 7-57
- set snmp usm on page 7-60
- show snmp community on page 7-89

set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device to which MSS sends SNMP notifications. You can configure the MSS SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

SNMPv3 with Informs

To configure a notification target for informs from SNMPv3, use the following command:

Syntax

set snmp notify target *target-num ip-addr*[:*udp-port-number*] **usm inform user** *username* **snmp-engine-id** {**ip** | **hex** *hex-string*} [**profile** *profile-name*] [**security** {**unsecured** | **authenticated** | **encrypted**}][**retries** *num*][**timeout** *num*]

Parameters

target-num	ID for the target. This ID is local to the RoamAbout switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
username	USM username. This option is applicable only when the SNMP version is **usm**. If the user will send informs rather than traps, you also must specify the **snmp-engine-id** of the target.
snmp-engine-id {**ip** | **hex** *hex-string*}	SNMP engine ID of the target. Specify **ip** if the target's SNMP engine ID is based on its IP address. If the target's SNMP engine ID is a hexadecimal value, use **hex** *hex-string* to specify the value.
profile *profile-name*	Notification profile this SNMP user will use to specify the notification types to send or drop.
security {**unsecured** | **authenticated** | **encrypted**}	Specifies the security level, and is applicable only when the SNMP version is **usm**: • **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default. • **authenticated**—Message exchanges are authenticated, but are not encrypted. • **encrypted**—Message exchanges are authenticated and encrypted.

retries *num*	Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
timeout *num*	Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv3 with Traps

To configure a notification target for traps from SNMPv3, use the following command:

Syntax

set snmp notify target *target-num ip-addr*[:*udp-port-number*] **usm trap user** *username* [**profile** *profile-name*] [**security** {**unsecured** | **authenticated** | **encrypted**}]

Parameters

target-num	ID for the target. This ID is local to the RoamAbout switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
username	USM username. This option is applicable only when the SNMP version is **usm**.
profile *profile-name*	Notification profile this SNMP user will use to specify the notification types to send or drop.
security {**unsecured** | **authenticated** | **encrypted**}	Specifies the security level, and is applicable only when the SNMP version is **usm**: • **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default. • **authenticated**—Message exchanges are authenticated, but are not encrypted. • **encrypted**—Message exchanges are authenticated and encrypted.

SNMPv2c with Informs

To configure a notification target for informs from SNMPv2c, use the following command:

Syntax

set snmp notify target *target-num ip-addr*[:*udp-port-number*] **v2c** *community-string* **inform** [**profile** *profile-name*] [**retries** *num*][**timeout** *num*]

Parameters

target-num	ID for the target. This ID is local to the RoamAbout switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
community-string	Community string.
profile *profile-name*	Notification profile this SNMP user will use to specify the notification types to send or drop.
retries *num*	Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
timeout *num*	Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv2c with Traps

To configure a notification target for traps from SNMPv2c, use the following command:

Syntax

set snmp notify target *target-num ip-addr*[:*udp-port-number*] **v2c** *community-string* **trap** [**profile** *profile-name*]

Parameters

target-num	ID for the target. This ID is local to the RoamAbout switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
community-string	Community string.
profile *profile-name*	Notification profile this SNMP user will use to specify the notification types to send or drop.

SNMPv1 with Traps

To configure a notification target for traps from SNMPv1, use the following command:

Syntax

set snmp notify target *target-num ip-addr*[:*udp-port-number*] **v1** *community-string* [**profile** *profile-name*]

Parameters

target-num	ID for the target. This ID is local to the RoamAbout switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
ip-addr[:*udp-port-number*]	IP address of the server. You also can specify the UDP port number to send notifications to.
community-string	Community string.
profile *profile-name*	Notification profile this SNMP user will use to specify the notification types to send or drop.

Defaults

The default UDP port number on the target is 162. The default minimum required security level is **unsecured**. The default number of retries is 0 and the default timeout is 2 seconds.

Mode

Enabled.

Usage

The **inform** or **trap** option specifies whether the MSS SNMP engine expects the target to acknowledge notifications sent to the target by the RoamAbout switch. Use **inform** if you want acknowledgements. Use **trap** if you do not want acknowledgements. The **inform** option is applicable to SNMP version **v2c** or **usm** only.

Examples

The following command configures a notification target for acknowledged notifications:

```
RBT-8100# set snmp notify target 1 10.10.40.9 usm inform user securesnmpmgr1
snmp-engine-id ip
success: change accepted.
```

This command configures target 1 at IP address 10.10.40.9. The target's SNMP engine ID is based on its address. The MSS SNMP engine will send notifications based on the default profile, and will require the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```
RBT-8100# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```

Related Commands

- clear snmp notify target on page 7-13
- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp profile on page 7-51
- set snmp protocol on page 7-56
- set snmp security on page 7-57
- set snmp usm on page 7-60
- show snmp notify target on page 7-92

set snmp profile

Configures an SNMP notification profile. A *notification profile* is a named list of all the notification types that can be generated by a switch, and for each notification type, the action to take (drop or send) when an event occurs.

You can configure up to ten notification profiles.

Syntax

set snmp profile {**default** | *profile-name*} {**drop** | **send**} {*notification-type* | **all**}

Parameters

default | *profile-name*	Name of the notification profile you are creating or modifying. The *profile-name* can be up to 32 alphanumeric characters long, with no spaces. To modify the default notification profile, specify **default**.
drop | **send**	Specifies the action that the SNMP engine takes with regard to the notifications you specify with *notification-type* or **all**.

notification-type	Name of the notification type: • **AuthenTraps**—Generated when the RoamAbout switch's SNMP engine receives a bad community string. • **AutoTuneRadioChannelChangeTraps**—Generated when the RF Auto-Tuning feature changes the channel on a radio. • **AutoTuneRadioPowerChangeTraps**—Generated when the RF Auto-Tuning feature changes the power setting on a radio. • **ClientAssociationFailureTraps**—Generated when a client's attempt to associate with a radio fails. • **ClientAuthorizationSuccessTraps**—Generated when a client is successfully authorized. • **ClientAuthenticationFailureTraps**—Generated when authentication fails for a client. • **ClientAuthorizationFailureTraps**—Generated when authorization fails for a client. • **ClientClearedTraps**—Generated when a client's session is cleared. • **ClientDeAssociationTraps**—Generated when a client is dissociated from a radio. • **ClientDot1xFailureTraps**—Generated when a client experiences an 802.1X failure. • **ClientRoamingTraps**—Generated when a client roams. • **CounterMeasureStartTraps**—Generated when MSS begins countermeasures against a rogue access point. • **CounterMeasureStopTraps**—Generated when MSS stops countermeasures against a rogue access point. • **DAPConnectWarningTraps**—Generated when a Distributed access point whose fingerprint has not been configured in MSS establishes a management session with the switch. • **DeviceFailTraps**—Generated when an event with an Alert severity occurs. • **DeviceOkayTraps**—Generated when a device returns to its normal state. • **LinkDownTraps**—Generated when the link is lost on a port. • **LinkUpTraps**—Generated when the link is detected on a port. • **MichaelMICFailureTraps**—Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures. • **MobilityDomainJoinTraps**—Generated when the RoamAbout switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.

notification-type (cont.)	• **MobilityDomainTimeoutTraps**—Generated when a timeout occurs after a RoamAbout switch has unsuccessfully tried to communicate with a seed member. • **APBootTraps**—Generated when an access point boots. • **APTimeoutTraps**—Generated when an access point fails to respond to the RoamAbout switch. • **PoEFailTraps**—Generated when a serious PoE problem, such as a short circuit, occurs. • **RFDetectAdhocUserTraps**—Generated when MSS detects an ad-hoc user. • **RFDetectRogueAPTraps**—Generated when MS detects a rogue access point. • **RFDetectRogueDisappearTraps**—Generated when a rogue access point is no longer being detected. • **RFDetectClientViaRogueWiredAPTraps**—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP. • **RFDetectDoSPortTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood. • **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood. • **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected. **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected. • **RFDetectClientViaRogueWiredAPTraps**—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP. • **RFDetectDoSPortTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood. • **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood. • **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected. • **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected. • **RFDetectSpoofedMacAPTraps**—Generated when MSS detects a wireless packet with the source MAC address of an Enterasys Networks access point, but without the spoofed access point's signature (fingerprint). • **RFDetectSpoofedSsidAPTraps**—Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.

notification-type (cont.)	• **RFDetectUnAuthorizedAPTraps**—Generated when MSS detects the MAC address of an AP that is on the attack list. • **RFDetectUnAuthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected. • **RFDetectUnAuthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.
all	Sends or drops all notifications.

Defaults

A default notification profile (named *default*) is already configured in MSS. All notifications in the default profile are dropped by default.

Mode

Enabled.

Examples

The following command changes the action in the default notification profile from **drop** to **send** for all notification types:

```
RBT-8100# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to **send** for all RF detection notification types:

```
RBT-8100# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectClientViaRogueWiredAPTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send RFDetectDoSTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueAPTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueDisappearTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send RFDetectRogueAPTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectRogueDisappearTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedMacAPTraps
success: change accepted.
```

```
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedSsidAPTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectUnAuthorizedAPTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectUnAuthorizedOuiTraps
success: change accepted.
RBT-8100# set snmp notify profile snmpprof_rfdetect send
RFDetectUnAuthorizedSsidTraps
success: change accepted.
```

Related Commands

- clear snmp notify profile on page 7-14
- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp notify target on page 7-46
- set snmp protocol on page 7-56
- set snmp security on page 7-57
- set snmp usm on page 7-60
- show snmp notify profile on page 7-91

set snmp protocol

Enables an SNMP protocol. MSS supports SNMPv1, SNMPv2c, and SNMPv3.

Syntax

```
set snmp protocol {v1 | v2c | usm | all} {enable | disable}
```

Parameters

v1	SNMPv1
v2c	SNMPv2c
usm	SNMPv3 (with the user security model)
all	Enables all supported versions of SNMP.
enable	Enables the specified SNMP version(s).
disable	Disables the specified SNMP version(s).

Defaults

All SNMP versions are disabled by default.

Mode

Enabled.

Usage

SNMP requires the switch's system IP address to be set. SNMP will not work without the system IP address.

You also must enable the SNMP service using the **set ip snmp server** command.

Example

The following command enables all SNMP versions:

```
RBT-8100# set snmp protocol all enable
success: change accepted.
```

Related Commands

- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp notify target on page 7-46
- set snmp profile on page 7-51
- set snmp security on page 7-57
- set snmp usm on page 7-60
- show snmp status on page 7-93

set snmp security

Sets the minimum level of security MSS requires for SNMP message exchanges.

Syntax

set snmp security {**unsecured** | **authenticated** | **encrypted** | **auth-req-unsec-notify**}

Parameters

unsecured	SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c.
authenticated	SNMP message exchanges are authenticated but are not encrypted.
encrypted	SNMP message exchanges are authenticated and encrypted.
auth-req-unsec-notify	SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted.

Defaults

By default, MSS allows nonsecure (**unsecured**) SNMP message exchanges.

Mode

Enabled.

Usage

SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to **unsecured**.

Example

The following command sets the minimum level of SNMP security allowed to authentication ***and*** encryption:

```
RBT-8100# set snmp security encrypted
success: change accepted.
```

Related Commands

- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp notify target on page 7-46
- set snmp profile on page 7-51
- set snmp protocol on page 7-56
- set snmp usm on page 7-60
- show snmp status on page 7-93

set snmp trap

This command is deprecated in MSS Version 4.0. To enable or disable SNMP notifications, configure a notification profile. See set snmp profile on page 7-51.

Enables or disables the SNMP trap capability. Traps are event notifications. When a trap condition occurs, the RoamAbout switch sends an SNMP trap message to any network management system specified as a trap receiver.

Syntax

set snmp trap {**enable** | **disable**} [*trap-name* | **all**]

Parameters

enable	Enables trap information to be sent.
disable	Disables the sending of trap information.
trap-name	Name of the trap:
all	Enables or disables all traps.

Defaults

All traps are disabled by default.

Mode

Enabled.

Usage

You can enable or disable the linkup and linkdown traps on an individual port basis with the **set port trap** command. The individual port setting overrides the global setting.

Examples

The following command disables all traps:

```
RBT-8100# set snmp trap disable all
success: change accepted.
```

The following command reenables authentication traps:

```
RBT-8100# set snmp trap enable AuthenTraps
success: change accepted.
```

Related Commands

- clear snmp trap receiver on page 7-15
- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp trap receiver on page 7-59
- show snmp configuration on page 7-87

set snmp trap receiver

This command is deprecated in MSS Version 4.0. To configure an SNMP notification target (also called *trap receiver*), see set snmp notify target on page 7-46.

Adds an IP address to the SNMP trap receiver table.

Syntax

set snmp trap receiver *ip-addr*

Parameters

ip-addr	IP address of the trap receiver, in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Example

To set the IP address of the SNMP trap receiver to 192.168.0.1, type the following command:

```
RBT-8100# set snmp trap receiver 192.168.0.1
success: change accepted.
```

Related Commands

- clear snmp trap receiver on page 7-15
- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp trap on page 7-58
- show snmp configuration on page 7-87

set snmp usm

Creates a USM user for SNMPv3.

Note: This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the **set snmp community** command to configure community strings.

Syntax

```
set snmp usm usm-username snmp-engine-id {ip ip-addr | local | hex hex-string}
access {read-only | read-notify | notify-only | read-write | notify-read-write}
auth-type {none | md5 | sha} {auth-pass-phrase string | auth-key hex-string}
encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase string |
encrypt-key hex-string}
```

Parameters

usm-username	Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces.
snmp-engine-id {**ip** *ip-addr* | **local** | **hex** *hex-string*}	Specifies a unique identifier for the SNMP engine. To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify **local** as the engine ID. • **hex** *hex-string*—ID is a hexadecimal string. • **ip** *ip-addr*—ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address. • **local**—Uses the value computed from the switch's system IP address.
access {**read-only** | **read-notify** | **notify-only** | **read-write** | **notify-read-write**}	Specifies the access level of the user: • **read-only**—An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them. • **read-notify**—An SNMP management application using the string can get object values on the switch but cannot set them. The switch can use the string to send notifications. • **notify-only**—The switch can use the string to send notifications. • **read-write**—An SNMP management application using the string can get and set object values on the switch. • **notify-read-write**—An SNMP management application using the string can get and set object values on the switch. The switch can use the string to send notifications.

auth-type {**none** | **md5** | **sha**} {**auth-pass-phrase** *string* | **auth-key** *hex-string*}	Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following: • **none**—No authentication is used. • **md5**—Message-digest algorithm 5 is used. • **sha**—Secure Hashing Algorithm (SHA) is used. If the authentication type is **md5** or **sha**, you can specify a passphrase or a hexadecimal key. • To specify a passphrase, use the **auth-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces. • To specify a key, use the **auth-key** *hex-string* option.
encrypt-type {**none** | **des** | **3des** | **aes**} {**encrypt-pass-phrase** *string* | **encrypt-key** *hex-string*}	Specifies the encryption type used for SNMP traffic. You can specify one of the following: • **none**—No encryption is used. This is the default. • **des**—Data Encryption Standard (DES) encryption is used. • **3des**—Triple DES encryption is used. • **aes**—Advanced Encryption Standard (AES) encryption is used. If the encryption type is **des**, **3des**, or **aes**, you can specify a passphrase or a hexadecimal key. • To specify a passphrase, use the **encrypt-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces. • To specify a key, use the **encrypt-key** *hex-string* option.

Defaults

No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is **read-only**, and the default authentication and encryption types are both **none**.

Mode

Enabled.

Examples

The following command creates USM user *snmpmgr1*, associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
RBT-8100# set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user *securesnmpmgr1*, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
RBT-8100# set snmp usm securesnmpmgr1 snmp-engine-id ip 192.168.40.2 auth-type
sha auth-pass-phrase myauthpword encrypt-type 3des encrypt-pass-phrase
mycryptpword
success: change accepted.
```

Related Commands

- clear snmp usm on page 7-16
- set ip snmp server on page 7-36
- set snmp community on page 7-44
- set snmp notify target on page 7-46
- set snmp profile on page 7-51
- set snmp protocol on page 7-56
- set snmp security on page 7-57
- show snmp usm on page 7-94

set summertime

Offsets the real-time clock of a RoamAbout switch by +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set.

Syntax

set summertime *summer-name* [**start** *week weekday month hour min* end *week weekday month hour min*]

Parameters

summer-name	Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like.
start	Start of the time change period.
week	Week of the month to start or end the time change. Valid values are **first**, **second**, **third**, **fourth**, or **last**.
weekday	Day of the week to start or end the time change. Valid values are **sun**, **mon**, **tue**, **wed**, **thu**, **fri**, and **sat**.
month	Month of the year to start or end the time change. Valid values are **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov**, and **dec**.
hour	Hour to start or end the time change—a value between 0 and 23 on the 24-hour clock.
min	Minute to start or end the time change—a value between 0 and 59.
end	End of the time change period.

Defaults

If you do not specify a start and end time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

Mode

Enabled.

Usage

You must first set the time zone with the **set timezone** command for the offset to work properly without the start and end values.

Configure summertime *before* you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

Example

To enable summertime and set the summertime time zone to *PDT* (Pacific Daylight Time), type the following command:

```
RBT-8100#  set summertime PDT
success: change accepted
```

Related Commands

- clear summertime on page 7-17
- clear timezone on page 7-19
- set timedate on page 7-66
- set timezone on page 7-67
- show summertime on page 7-95
- show timedate on page 7-96
- show timezone on page 7-97

set system ip-address

Configures the system IP address. The system IP address determines the interface or source IP address MSS uses for system tasks, including the following:

- Mobility domain operations
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Syntax

set system ip-address *ip-addr*

Parameters

ip-addr	IP address, in dotted decimal notation. The address must be configured on one of the RoamAbout switch's VLANs.

Defaults

None.

Mode

Enabled.

Usage

You must use an address that is configured on one of the RoamAbout switch's VLANs.

To display the system IP address, use the **show system** command.

Example

The following commands configure an IP interface on VLAN *taupe* and configure the interface to be the system IP address:

```
RBT-8100# set interface taupe ip 10.10.20.20/24
success: set ip address 10.10.20.20 netmask 255.255.255.0 on vlan taupe
RBT-8100# set system ip-address 10.10.20.20
success: change accepted.
```

Related Commands

- clear system ip-address on page 7-18
- set interface on page 7-24
- show system on page 3-26

set timedate

Sets the time of day and date on the RoamAbout switch.

Syntax

```
set timedate {date mmm dd yyyy [time hh:mm:ss]}
```

Parameters

date *mmm dd yyyy*	System date: • *mmm*—month. • *dd*—day. • *yyyy*—year.
time *hh:mm:ss*	System time, in hours, minutes, and seconds.

Defaults

None.

Mode

Enabled.

Usage

The day of week is automatically calculated from the day you set. The time displayed by the CLI after you type the command might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.

Configure summertime *before* you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

Example

The following command sets the date to March 13, 2003 and time to 11:11:12:

```
RBT-8100# set timedate date feb 29 2004 time 23:58:00
Time now is: Sun Feb 29 2004, 23:58:02 PST
```

Related Commands

- clear summertime on page 7-17
- clear timezone on page 7-19
- set summertime on page 7-63
- set timezone on page 7-67
- show summertime on page 7-95
- show timedate on page 7-96
- show timezone on page 7-97

set timezone

Sets the number of hours, and optionally the number of minutes, that the RoamAbout switch's real-time clock is offset from Coordinated Universal Time (UTC). These values are also used by Network Time Protocol (NTP), if it is enabled.

Syntax

set timezone *zone-name* {*-hours* [*minutes*]}

Parameters

zone-name	Time zone name of up to 32 alphabetic characters. You can use a standard name or any name you like.
-	Minus time to indicate hours (and minutes) to be subtracted from UTC. Otherwise, hours and minutes are added by default.
hours	Number of hours to add or subtract from UTC.
minutes	Number of minutes to add or subtract from UTC.

Defaults

If this command is not used, then the default time zone is UTC.

Mode

Enabled.

Example

To set the time zone for Pacific Standard Time (PST), type the following command:

```
RBT-8100#  set timezone PST -8
Timezone is set to 'PST', offset from UTC is -8:0 hours.
```

Related Commands

- clear summertime on page 7-17
- clear timezone on page 7-19
- set summertime on page 7-63
- set timedate on page 7-66
- show summertime on page 7-95
- show timedate on page 7-96
- show timezone on page 7-97

show arp

Displays the ARP table.

Syntax

show arp [*ip-addr*]

Parameters

ip-addr	IP address.

Defaults

If you do not specify an IP address, the whole ARP table is displayed.

Mode

All.

Example

The following command displays ARP entries:

```
RBT-8100# show arp
ARP aging time: 1200 seconds

Host                           HW Address         VLAN  Type    State
------------------------------ ----------------- ----- ------- --------
10.5.4.51                      00:0b:0e:02:76:f5     1 DYNAMIC RESOLVED
10.5.4.53                      00:0b:0e:02:76:f7     1 LOCAL   RESOLVED
```

Table 7-1 describes the fields in this display.

Table 7-1 Output for show arp

Field	Description
ARP aging time	Number of seconds a dynamic entry can remain unused before MSS removes the entry from the ARP table.
Host	IP address, hostname, or alias.
HW Address	MAC address mapped to the IP address, hostname, or alias.
VLAN	VLAN the entry is for.

Table 7-1 Output for show arp (continued)

Field	Description
Type	Entry type: • DYNAMIC—Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout. • LOCAL—Entry for the RoamAbout switch MAC address. Each VLAN has one local entry for the switch MAC address. • PERMANENT—Entry does not age out and remains in the configuration even following a reboot. • STATIC—Entry does not age out but is removed after a reboot.
State	Entry state: • RESOLVING—MSS sent an ARP request for the entry and is waiting for the reply. • RESOLVED—Entry is resolved.

Related Commands

- set arp on page 7-22
- set arp agingtime on page 7-23

show dhcp-client

Displays DHCP client information for all VLANs.

Syntax

```
show dhcp-client
```

Parameters

None.

Defaults

None.

Mode

All.

Example

The following command displays DHCP client information:

```
RBT-8100# show dhcp-client
 Interface:            corpvlan(4)
 Configuration Status: Enabled
 DHCP State:           IF_UP
 Lease Allocation:     65535 seconds
 Lease Remaining:      65532 seconds
 IP Address:           10.3.1.110
 Subnet Mask:          255.255.255.0
 Default Gateway:      10.3.1.1
 DHCP Server:          10.3.1.4
 DNS Servers:          10.3.1.29
 DNS Domain Name:      mycorp.com
```

Table 7-2 describes the fields in this display.

Table 7-2 Output for show dhcp-client

Output	What it displays...
Interface	VLAN name and number.
Configuration Status	Status of the DHCP client on this VLAN: • Enabled • Disabled
DHCP State	State of the IP interface: • IF_UP • IF_DOWN
Lease Allocation	Duration of the address lease.
Lease Remaining	Number of seconds remaining before the address lease expires.
IP Address	IP address received from the DHCP server.

Table 7-2 Output for show dhcp-client (continued)

Output	What it displays...
Subnet Mask	Network mask of the IP address received from the DHCP server.
Default Gateway	Default router IP address received from the DHCP server. If the address is 0.0.0.0, the server did not provide an address.
DHCP Server	IP address of the DHCP server.
DNS Servers	DNS server IP address(es) received from the DHCP server.
DNS Domain Name	Default DNS domain name received from the DHCP server.

Related Commands

set interface dhcp-client on page 7-25

show dhcp-server

Displays MSS DHCP server information.

Syntax

show dhcp-server [**interface** *vlan-id*] [**verbose**]

Parameters

interface *vlan-id*	Displays the IP addresses leased by the specified VLAN.
verbose	Displays configuration and status information for the MSS DHCP server.

Defaults

None.

Mode

All.

Examples

The following command displays the addresses leased by the MSS DHCP server:

```
RBT-8100# show dhcp-server
VLAN Name            Address         MAC                Lease Remaining (sec)
---- --------------- --------------- ------------------ --------------------
   1 default         10.10.20.2      00:01:02:03:04:05                  12345
   1 default         10.10.20.3      00:01:03:04:06:07                   2103
   2 red-vlan        192.168.1.5     00:01:03:04:06:08                    102
   2 red-vlan        192.168.1.7     00:01:03:04:06:09                  16789
```

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
RBT-8100# show dhcp-server verbose
Interface:        0 (Direct AP)
 Status:           UP
 Address Range:    10.0.0.1-10.0.0.253

 Interface:            default(1)
 Status:               UP
 Address Range:        10.10.20.2-10.10.20.254
   Hardware Address:     00:01:02:03:04:05
   State:                BOUND
   Lease Allocation:     43200 seconds
```

```
Lease Remaining:      12345 seconds
IP Address:           10.10.20.2
Subnet Mask:          255.255.255.0
Default Router:      10.10.20.1
DNS Servers:          10.10.20.4 10.10.20.5
DNS Domain Name:      mycorp.com
```

Table 7-3 and Table 7-4 describe the fields in these displays.

Table 7-3 Output for show dhcp-server

Output	What it displays...
VLAN	VLAN number.
Name	VLAN name.
Address	IP address leased by the server.
MAC Address	MAC address of the device that holds the lease for the address.
Lease Remaining	Number of seconds remaining before the address lease expires.

Table 7-4 Output for show dhcp-client verbose

Output	What it displays...
Interface	VLAN name and number.
Status	Status of the interface: • UP • DOWN
Address Range	Range from which the server can lease addresses.
Hardware Address	MAC address of the DHCP client.
State	State of the address lease: • SUSPEND—MSS is checking for the presence of another DHCP server on the subnet. This is the initial state of the MSS DHCP server. The MSS DHCP server remains in this state if another DHCP server is detected. • CHECKING—MSS is using ARP to verify whether the address is available. • OFFERING—MSS offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address. • BOUND—The client accepted the address. • HOLDING—The address is already in use and is therefore unavailable.
Lease Allocation	Duration of the address lease, in seconds.
Lease Remaining	Number of seconds remaining before the address lease expires.
IP Address	IP address leased to the client.
Subnet Mask	Network mask of the IP address leased to the client.
Default Router	Default router IP address included in the DHCP Offer to the client.

Table 7-4 Output for show dhcp-client verbose (continued)

Output	What it displays...
DNS Servers	DNS server IP address(es) included in the DHCP Offer to the client.
DNS Domain Name	Default DNS domain name included in the DHCP Offer to the client.

Related Commands

set interface dhcp-server on page 7-26

show interface

Displays the IP interfaces configured on the RoamAbout switch.

Syntax

show interface [*vlan-id*]

Parameters

vlan-id	VLAN name or number.

Defaults

If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

Mode

All.

Usage

The IP interface table flags an address assigned by a DHCP server with an asterisk (*).

Example

The following command displays all the IP interfaces configured on a RoamAbout switch:

```
RBT-8100# show interface
VLAN Name            Address         Mask            Enabled State RIB
---- --------------- --------------- --------------- ------- ----- ---------
   1 default         10.10.10.10     255.255.255.0   YES     Up    ipv4
   2 mauve           10.10.20.10     255.255.255.0   NO      Down  ipv4
   4 corpvlan       *10.3.1.110      255.255.255.0   YES     Up    ipv4
```

Table 7-5 describes the fields in this display.

Table 7-5 Output for show interface

Output	What it displays...
VLAN	VLAN number
Name	VLAN name
Address	IP address
Mask	Subnet mask
Enabled	Administrative state: • YES (enabled) • NO (disabled)

Table 7-5 Output for show interface (continued)

Output	What it displays...
State	Link state: • Up (operational) • Down (unavailable)
RIB	Routing Information Base

Related Commands

- clear interface on page 7-4
- set interface on page 7-24
- set interface status on page 7-28

show ip alias

Displays the IP aliases configured on the RoamAbout switch.

Syntax

show ip alias [*name*]

Parameters

name	Alias string.

Defaults

If you do not specify an alias name, all aliases are displayed.

Mode

Enabled.

Example

The following command displays all the aliases configured on a RoamAbout switch:

```
RBT-8100# show ip alias
Name                    IP Address
--------------------    --------------------
HR1                     192.168.1.2
payroll                 192.168.1.3
radius1                 192.168.7.2
```

Table 7-6 describes the fields in this display.

Table 7-6 Output for show ip alias

Output	What it displays...
Name	Alias string.
IP Address	IP address associated with the alias.

Related Commands

- clear ip alias on page 7-5
- set ip alias on page 7-29

show ip dns

Displays the DNS servers the RoamAbout switch is configured to use.

Syntax

show ip dns

Parameters

None.

Defaults

None.

Mode

All.

Example

The following command displays the DNS information:

```
RBT-8100# show ip dns
Domain Name: example.com
DNS Status: enabled
IP Address                Type
-----------------------------------
10.1.1.1                  PRIMARY
10.1.1.2                  SECONDARY
10.1.2.1                  SECONDARY
```

Table 7-7 describes the fields in this display.

Table 7-7 Output for show ip dns

Output	What it displays...
Domain Name	Default domain name configured on the RoamAbout switch
DNS Status	Status of the switch's DNS client: • Enabled • Disabled
IP Address	IP address of the DNS server
Type	Server type: • PRIMARY • SECONDARY

Related Commands

- clear ip dns domain on page 7-6
- clear ip dns server on page 7-7

- set ip dns on page 7-30
- set ip dns domain on page 7-31
- set ip dns server on page 7-32

show ip https

Displays information about the HTTPS management port.

Syntax

show ip https

Parameters

None.

Defaults

None.

Mode

All.

Example

The following command shows the status and port number for the HTTPS management interface to the RoamAbout switch:

```
RBT-8100> show ip https
HTTPS is enabled
HTTPS is set to use port 443

Last 10 Connections:
 IP Address     Last Connected          Time Ago (s)
------------    ---------------------- ------------
10.10.10.56     2003/05/09 15:51:26 pst          349
```

Table 7-8 describes the fields in this display.

Table 7-8 Output for show ip https

Output	What it displays...
HTTPS is enabled/disabled	State of the HTTPS server: • Enabled • Disabled
HTTPS is set to use port	TCP port number on which the RoamAbout switch listens for HTTPS connections.
Last 10 connections	List of the last 10 devices to establish connections to the RoamAbout switch's HTTPS server.
IP Address	IP address of the device that established the connection. **Note:** If a browser connects to a RoamAbout switch from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output.
Last Connected	Time when the device established the HTTPS connection to the switch.

Table 7-8 Output for show ip https (continued)

Output	What it displays...
Time Ago (s)	Number of seconds since the device established the HTTPS connection to the switch.

Related Commands

- clear ip telnet on page 7-9
- set ip https server on page 7-33
- set ip telnet on page 7-39
- set ip telnet server on page 7-40
- show ip telnet on page 7-84

show ip route

Displays the IP route table.

Syntax

show ip route [*destination*]

Parameters

destination	Route destination IP address, in dotted decimal notation.

Defaults

None.

Mode

All.

Usage

When you add an IP interface to a VLAN that is up, MSS adds direct and local routes for the interface to the route table. If the VLAN is down, MSS does not add the routes. If you add an interface to a VLAN but the routes for that interface do not appear in the route table, use the **show vlan config** command to check the VLAN state.

If you add a static route and the route's state is shown as Down, use the **show interface** command to verify that the RoamAbout switch has an IP interface in the default router's subnet. MSS cannot resolve a static route unless one of the switch's VLANs has an interface in the default router's subnet. If the switch has such an interface but the static route is still down, use the **show vlan config** command to check the state of the VLAN's ports.

Example

The following command shows all routes in a RoamAbout switch's IP route table:

```
RBT-8100# show ip route
Router table for IPv4
Destination/Mask   Proto   Metric NH-Type Gateway         VLAN:Interface
_________________ _______ ______ _______ _______________ _______________

        0.0.0.0/ 0 Static       1 Router  10.0.1.17       Down
        0.0.0.0/ 0 Static       2 Router  10.0.2.17       vlan:2:ip
       10.0.2.1/24 IP           0 Direct                  vlan:2:ip
       10.0.2.1/32 IP           0 Direct                  vlan:2:ip:10.0.1.1/24
     10.0.2.255/32 IP           0 Direct                  vlan:2:ip:10.0.1.1/24
      224.0.0.0/ 4 IP           0 Local                   MULTICAST
```

Table 7-9 describes the fields in this display.

Table 7-9 Output for show ip route

Output	What it displays...
Destination/Mask	IP address and subnet mask of the route destination. The 244.0.0.0 route is automatically added by MSS and supports the IGMP snooping feature.
Proto	Protocol that added the route to the IP route table. The protocol can be one of the following: • IP—MSS added the route. • Static—An administrator added the route.
Metric	Cost for using the route.
NH-Type	Next-hop type: • Local—Route is for a local interface. MSS adds the route when you configure an IP address on the RoamAbout switch. • Direct—Route is for a locally attached subnet. MSS adds the route when you add an interface in the same subnet to the RoamAbout switch. • Router—Route is for a remote destination. A RoamAbout switch forwards traffic for the destination to the default router (gateway).
Gateway	Next-hop router for reaching the route destination. **Note:** This field applies only to static routes.
VLAN:Interface	Destination VLAN, protocol type, and IP address of the route. Because direct routes are for local interfaces, a destination IP address is not listed. The destination for the IP multicast route is MULTICAST. For static routes, the value Down means the RoamAbout switch does not have an interface to the destination's next-hop router. To provide an interface, configure an IP interface that is in the same IP subnet as the next-hop router. The IP interface must be on a VLAN containing the port that is attached to the default router.

Related Commands

- clear ip route on page 7-8
- set interface on page 7-24
- set ip route on page 7-34
- show interface on page 7-75
- show vlan config on page 5-24

show ip telnet

Displays information about the Telnet management port.

Syntax

```
show ip telnet
```

Parameters

None.

Defaults

None.

Mode

All.

Example

The following command shows the status and port number for the Telnet management interface to the RoamAbout switch:

```
RBT-8100> show ip telnet

Server Status                 Port
-----------------------------------
Enabled                        23
```

Table 7-10 describes the fields in this display.

Table 7-10 Output for show ip telnet

Output	What it displays...
Server Status	State of the HTTPS server: • Enabled • Disabled
Port	TCP port number on which the RoamAbout switch listens for Telnet management traffic.

Related Commands

- clear ip telnet on page 7-9
- set ip https server on page 7-33
- set ip telnet on page 7-39
- set ip telnet server on page 7-40
- show ip https on page 7-80

show ntp

Displays NTP client information.

Syntax

show ntp

Parameters

None.

Defaults

None.

Mode

All.

Example

To display NTP information for a RoamAbout switch, type the following command:

```
RBT-8100> show ntp
NTP client: enabled
Current update-interval: 20(secs)
Current time: Fri Feb 06 2004, 12:02:57
Timezone is set to 'PST', offset from UTC is -8:0 hours.
Summertime is enabled.
Last NTP update: Fri Feb 06 2004, 12:02:46
NTP Server          Peer state          Local State
-------------------------------------------------
192.168.1.5         SYSPEER             SYNCED
```

Table 7-11 describes the fields in this display.

Table 7-11 Output for show ntp

Output	What it displays...
NTP client	State of the NTP client. The state can be one of the following: • Enabled • Disabled
Current update-interval	Number of seconds between queries sent by the RoamAbout switch to the NTP servers for updates.
Current time	System time that was current on the RoamAbout switch when you pressed Enter after typing the **show ntp** command.
Timezone	Time zone configured on the switch. MSS offsets the time reported by the NTP server based on the time zone. **Note:** This field is displayed only if you change the time zone.

Table 7-11 Output for show ntp (continued)

Output	What it displays...
Summertime	Summertime period configured on the switch. MSS offsets the system time +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set. **Note:** This field is displayed only if you enable summertime.
Last NTP update	Time when the switch received the most recent update from an NTP server.
NTP Server	IP address of the NTP server.
Peer state	State of the NTP session from the point of view of the NTP server: • CORRECT • REJECT • SELCAND • SYNCCAND • SYSPEER
Local state	State of the NTP session from the point of view of the RoamAbout switch's NTP client: • INITED • START • SYNCED

Related Commands

- clear ntp server on page 7-10
- clear summertime on page 7-17
- clear timezone on page 7-19
- set ntp on page 7-41
- set ntp server on page 7-42
- set summertime on page 7-63
- set timezone on page 7-67
- show timezone on page 7-97

show snmp configuration

This command is deprecated in MSS Version 4.0. Use the **show snmp status** command instead.

Shows SNMP settings on a RoamAbout switch.

Syntax

show snmp configuration

Parameters

None.

Defaults

None.

Mode

All.

Example

To display SNMP settings on a RoamAbout switch, type the following command:

```
RBT-8100#  show snmp configuration
Snmp agent is enabled
System Name: RBT-8100
System location:
System contact:

     Trap Name                          Enabled
     ---------------------------------  -------
     LinkDownTraps                      YES
     LinkUpTraps                        YES
     AuthenTraps                        YES
     DeviceFailTraps                    YES
     DeviceOkayTraps                    YES
     PoEFailTraps                       YES
     APTimeoutTraps                     YES
     APBootTraps                        YES
     MobilityDomainJoinTraps            YES
     MobilityDomainTimeoutTraps         YES
     MichaelMICFailureTraps             YES
     RFDetectRogueAPTraps               YES
     RFDetectAdhocUserTraps             YES
     RFDetectRogueDisappearTraps        YES
     ClientAuthenticationFailureTraps   YES
     ClientAuthorizationFailureTraps    YES
     ClientAssociationFailureTraps      YES
     ClientAuthorizationSuccessTraps    YES
     ClientClearedTraps                 YES
     ClientDeAssociationTraps           YES
```

```
ClientRoamingTraps                    YES
AutoTuneRadioPowerChangeTraps         YES
AutoTuneRadioChannelChangeTraps       YES
CounterMeasureStartTraps              YES
CounterMeasureStopTraps               YES
ClientDot1xFailureTraps               YES

Community Access    Community Name
----------------    --------------
read-only           public
read-write          private
```

Table 7-12 describes the fields in this display.

Table 7-12 Output for show snmp configuration

Output	What it displays...
Snmp agent is	State of the SNMP agent on the switch:
System Name	String configured by the **set system name** command.
System location	String configured by the **set system location** command.
System contact	String configured by the **set system contact** command.
System description	RoamAbout switch model.
Trap Receiver	IP address of each trap receiver.
Trap Name	SNMP traps supported by MSS.
Enabled	State of each trap:
Community Access	Type of access for an SNMP community.
Community Name	SNMP community name.

Related Commands

- set ip snmp server on page 7-36
- set port trap on page 4-25
- set snmp community on page 7-44
- set snmp trap on page 7-58
- set snmp trap receiver on page 7-59
- set system contact on page 3-15
- set system location on page 3-21
- set system name on page 3-22

show snmp community

Displays the configured SNMP community strings.

Syntax

```
show snmp community
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

To display the configured SNMP community strings, use the following command:

```
show snmp community
```

Related Commands

- clear snmp community on page 7-12
- set snmp community on page 7-44

show snmp counters

Displays SNMP statistics counters.

Syntax

```
show snmp counters
```

Parameters

None.

Defaults

None.

Mode

Enabled.

show snmp notify profile

Displays SNMP notification profiles.

Syntax

```
show snmp notify profile
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Related Commands

- clear snmp notify profile on page 7-14
- set snmp profile on page 7-51

show snmp notify target

Displays SNMP notification targets.

Syntax

```
show snmp notify target
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Related Commands

- clear snmp notify target on page 7-13
- set snmp notify target on page 7-46

show snmp status

Displays SNMP version and status information.

Syntax

```
show snmp status
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Related Commands

- set snmp community on page 7-44
- set snmp notify target on page 7-46
- set snmp profile on page 7-51
- set snmp protocol on page 7-56
- set snmp security on page 7-57
- set snmp usm on page 7-60
- show snmp community on page 7-89
- show snmp counters on page 7-90
- show snmp notify profile on page 7-91
- show snmp notify target on page 7-92
- show snmp usm on page 7-94

show snmp usm

Displays information about SNMPv3 users.

Defaults

None.

Mode

Enabled.

Related Commands

- clear snmp usm on page 7-16
- show snmp usm on page 7-94

show summertime

Shows a RoamAbout switch's offset from its real-time clock.

Syntax

show summertime

Parameters

None.

Defaults

There is no summertime offset by default.

Mode

All.

Example

To display the summertime setting on a RoamAbout switch, type the following command:

```
RBT-8100#  show summertime
Summertime is enabled, and set to 'PDT'.
  Start  : Sun Apr 04 2004, 02:00:00
  End    : Sun Oct 31 2004, 02:00:00
  Offset : 60 minutes
  Recurring : yes, starting at 2:00 am of first Sunday of April
              and ending at 2:00 am on last Sunday of October.
```

Related Commands

- clear summertime on page 7-17
- clear timezone on page 7-19
- set summertime on page 7-63
- set timedate on page 7-66
- set timezone on page 7-67
- show timedate on page 7-96
- show timezone on page 7-97

show timedate

Shows the date and time of day currently set on a RoamAbout switch's real-time clock.

Syntax

show timedate

Parameters

None.

Defaults

None.

Mode

All.

Example

To display the time and date set on a RoamAbout switch's real-time clock, type the following command:

```
RBT-8100#  show timedate
Sun Feb 29 2004, 23:59:02 PST
```

Related Commands

- clear summertime on page 7-17
- clear timezone on page 7-19
- set summertime on page 7-63
- set timedate on page 7-66
- set timezone on page 7-67
- show summertime on page 7-95
- show timezone on page 7-97

show timezone

Shows the time offset for the real-time clock from UTC on a RoamAbout switch.

Syntax

show timezone

Parameters

None.

Defaults

None.

Mode

All.

Example

To display the offset from UTC, type the following command:

```
RBT-8100# show timezone
Timezone set to 'pst', offset from UTC is -8 hours
```

Related Commands

- clear summertime on page 7-17
- clear timezone on page 7-19
- set summertime on page 7-63
- set timedate on page 7-66
- set timezone on page 7-67
- show summertime on page 7-95
- show timedate on page 7-96

telnet

Opens a Telnet client session with a remote device.

Syntax

telnet {*ip-addr* | *hostname*} [**port** *port-num*]

Parameters

ip-addr	IP address of the remote device.
hostname	Hostname of the remote device.
port *port-num*	TCP port number on which the TCP server on the remote device listens for Telnet connections.

Defaults

MSS attempts to establish Telnet connections with TCP port 23 by default.

Mode

Enabled.

Usage

To end a Telnet session from the remote device, press Ctrl+t or type **exit** in the management session on the remote device. To end a client session from the local device, use the **clear sessions telnet client** command.

If the configuration of the RoamAbout switch from which you enter the **telnet** command has an ACL that denies Telnet client traffic, the ACL also denies access by the **telnet** command.

Example

In the following example, an administrator establishes a Telnet session with another RoamAbout switch and enters a command on the remote switch:

```
RBT-8100# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^t'

Copyright (c) 2002, 2003
Enterasys Networks, Inc.

Username: username
Password: password
RBT-8100-remote> show vlan
                     Admin  VLAN  Tunl                          Port
VLAN Name            Status State Affin Port             Tag   State
---- --------------- ------ ----- ----- ---------------- ----- -----
   1 default         Up     Up        5
                                        1                 none Up
   3 red             Up     Up        5
```

```
  10 backbone          Up      Up         5
                                            21                 none Up
                                            22                 none Up
4094 web-aaa           Up      Up         0
                                            2                  4094 Up
```

When the administrator presses Ctrl+t to end the Telnet connection, the management session returns to the local RoamAbout switch prompt:

```
RBT-8100-remote> Session 0 pty tty2.d terminated tt name tty2.d
RBT-8100#
```

Related Commands

- clear sessions on page 18-2
- show sessions on page 18-5

traceroute

Traces the route to an IP host.

Syntax

traceroute *host* [**dnf**] [**no-dns**] [**port** *port-num*] [**queries** *num*] [**size** *size*] [**ttl** *hops*] [**wait** *ms*]

Parameters

host	IP address, hostname, or alias of the destination host. Specify the IP address in dotted decimal notation.
dnf	Sets the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented.
no-dns	Prevents MSS from performing a DNS lookup for each hop to the destination host.
port *port-num*	TCP port number listening for the traceroute probes.
queries *num*	Number of probes per hop.
size *size*	Probe packet size in bytes. You can specify from 40 through 1460.
ttl *hops*	Maximum number of hops, which can be from 1 through 255.
wait *ms*	Probe wait in milliseconds. You can specify from 1 through 100,000.

Defaults

- **dnf**—Disabled
- **no-dns**—Disabled
- **port**—33434
- **queries**—3
- **size**—38
- **ttl**—30
- **wait**—5000

Mode

All.

Usage

To stop a **traceroute** command that is in progress, press Ctrl+C.

Example

The following example traces the route to host *server1*:

```
RBT-8100# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
3 gateway_a.example.com (192.168.1.201) 6 ms 3 ms 3 ms
4 server1.example.com (192.168.22.7) 3 ms * 2 ms
```

The first row of the display indicates the target host, the maximum number of hops, and the packet size. Each numbered row displays information about one hop. The rows are displayed in the order in which the hops occur, beginning with the hop closest to the RoamAbout switch.

The row for a hop lists the total time in milliseconds for each ICMP packet to reach the router or host, plus the time for the ICMP *Time Exceeded* message to return to the host.

An exclamation point (!) following any of these values indicates that the *Port Unreachable* message returned by the destination has a maximum hop count of 0 or 1. This can occur if the destination uses the maximum hop count value from the arriving packet as the maximum hop count in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute packet with a maximum hop count equal to the number of hops between the source and destination.

An asterisk (*) indicates that the timeout period expired before MSS received a *Time Exceeded* message for the packet.

If Traceroute receives an ICMP error message other than a *Time Exceeded* or *Port Unreachable* message, MSS displays one of the error codes described in Table 7-13 instead of displaying the round-trip time or an asterisk (*).

Table 7-13 describes the **traceroute** error messages.

Table 7-13 Error Messages for traceroute

Output	What it displays...
!N	No route to host. The network is unreachable.
!H	No route to host. The host is unreachable.
!P	Connection refused. The protocol is unreachable.
!F	Fragmentation needed but Do Not Fragment (DNF) bit was set.
!S	Source route failed.
!A	Communication administratively prohibited.
?	Unknown error occurred.

Related Commands

ping on page 7-20

8

AAA Commands

Use authentication, authorization, and accounting (AAA) commands to provide a secure network connection and a record of user activity. Location policy commands override any virtual LAN (VLAN) or security ACL assignment by AAA or the local RAS database to help you control access locally.

(Security ACLs are packet filters. For command descriptions, see Chapter 14, **Security ACL Commands**.)

This chapter presents AAA commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear accounting	8-3
clear authentication admin	8-4
clear authentication console	8-5
clear authentication dot1x	8-6
clear authentication mac	8-7
clear authentication proxy	8-8
clear location policy	8-10
clear mac-user	8-11
clear mac-user attr	8-12
clear mac-user group	8-13
clear mac-usergroup	8-14
clear mac-usergroup attr	8-15
clear mobility-profile	8-16
clear user	8-17
clear user attr	8-18
clear user group	8-19
clear usergroup	8-20
clear usergroup attr	8-21
set accounting {admin | console}	8-22
set accounting {dot1x | mac | web | last-resort}	8-24

For information about...	Refer to page...
set accounting system	8-26
set authentication admin	8-27
set authentication console	8-29
set authentication dot1x	8-31
set authentication mac	8-35
set authentication proxy	8-37
set authentication web	8-38
set location policy	8-38
set location policy	8-38
set mac-user	8-43
set mac-user attr	8-44
set mac-usergroup attr	8-50
set mobility-profile	8-52
set mobility-profile mode	8-54
set user	8-55
set user attr	8-57
set user group	8-58
set usergroup	8-59
set web-portal	8-61
show aaa	8-62
show accounting statistics	8-65
show mobility-profile	8-69
set location policy	8-40
show location policy	8-68

clear accounting

Removes accounting services for specified wireless users with administrative access or network access.

Syntax

clear accounting {**admin** | **dot1x** | **system**} {*user-glob*}

Parameters

admin	Users with administrative access to the RAS through a console connection or through a Telnet or Web View connection.
dot1x	Users with network access through the RAS. Users with network access are authorized to use the network through either an IEEE 802.1X method or their media access control (MAC) address.
system	Disables sending of Accounting-On and Accounting-Off messages to a RADIUS server, if previously enabled. When this command is entered, an Accounting-Off message is generated and sent to the server or server group specified with the **set accounting system** command.
user-glob	Single user or set of users with administrative access or network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)

Default

None.

Mode

Enabled.

Example

The following command removes accounting services for authorized network user Nin:

```
RBT-8100# clear accounting dot1x Nin
success: change accepted.
```

Related Commands

- set accounting {admin | console} on page 8-22
- set accounting system on page 8-26
- show accounting statistics on page 8-65

clear authentication admin

Removes an authentication rule for administrative access through Telnet or Web View.

Syntax

clear authentication admin *user-glob*

Parameters

user-glob	A single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)

Default

None.

Mode

Enabled.

Note: The syntax descriptions for the **clear authentication** commands have been separated for clarity. However, the options and behavior for the **clear authentication admin** command are the same as in previous releases.

Example

The following command clears authentication for administrator Jose:

```
RBT-8100# clear authentication admin Jose
success: change accepted.
```

Related Commands

- clear authentication console on page 8-5
- clear authentication dot1x on page 8-6
- clear authentication web on page 8-9
- set authentication admin on page 8-27
- show aaa on page 8-62

clear authentication console

Removes an authentication rule for administrative access through the Console.

Syntax

clear authentication console *user-glob*

Parameters

user-glob	A single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)

Default

None.

Mode

Enabled.

Note: The syntax descriptions for the **clear authentication** commands have been separated for clarity. However, the options and behavior for the **clear authentication console** command are the same as in previous releases.

Example

The following command clears authentication for administrator Regina:

```
RBT-8100# clear authentication console Regina
success: change accepted.
```

Related Commands

- clear authentication admin on page 8-4
- clear authentication dot1x on page 8-6
- clear authentication mac on page 8-7
- clear authentication web on page 8-9
- set authentication console on page 8-29
- show aaa on page 8-62

clear authentication dot1x

Removes an 802.1X authentication rule.

Syntax

clear authentication dot1x {**ssid** *ssid-name* | **wired**} *user-glob*

Parameters

ssid *ssid-name*	SSID name to which this authentication rule applies.
wired	Clears a rule used for access over a RoamAbout switch's wired-authentication port.
user-glob	User-glob associated with the rule you are removing.

Default

None.

Mode

Enabled.

Example

The following command removes 802.1X authentication for network users with usernames ending in *@thiscorp.com* who try to access SSID *finance*:

```
RBT-8100# clear authentication dot1x ssid finance *@thiscorp.com
```

Related Commands

- clear authentication admin on page 8-4
- clear authentication console on page 8-5
- clear authentication mac on page 8-7
- clear authentication web on page 8-9
- set authentication dot1x on page 8-31
- show aaa on page 8-62

clear authentication mac

Removes a MAC authentication rule.

Syntax

clear authentication mac {**ssid** *ssid-name* | **wired**} *mac-addr-glob*

Parameters

ssid *ssid-name*	SSID name to which this authentication rule applies.
wired	Clears a rule used for access over a RoamAbout switch's wired-authentication port.
mac-addr-glob	MAC address glob associated with the rule you are removing.

Default

None.

Mode

Enabled.

Example

The following command removes a MAC authentication rule for access to SSID *thatcorp* by MAC addresses beginning with *aa:bb:cc:*

```
RBT-8100# clear authentication mac ssid thatcorp aa:bb:cc:*
```

Related Commands

- clear authentication admin on page 8-4
- clear authentication console on page 8-5
- clear authentication dot1x on page 8-6
- clear authentication web on page 8-9
- set authentication mac on page 8-35
- show aaa on page 8-62

clear authentication proxy

Removes a proxy rule for third-party AP users.

Syntax

clear authentication proxy ssid *ssid-name user-glob*

Parameters

ssid *ssid-name*	SSID name to which this authentication rule applies.
user-glob	User-glob associated with the rule you are removing.

Default

None.

Mode

Enabled.

Example

The following command removes the proxy rule for SSID *mycorp* and userglob **:

```
RBT-8100# clear authentication proxy ssid mycorp **
```

Related Commands

- set authentication proxy on page 8-37
- show aaa on page 8-62

clear authentication web

Removes a WebAAA rule.

Syntax

clear authentication web {**ssid** *ssid-name* | **wired**} *user-glob*

Parameters

ssid ssid-name	SSID name to which this authentication rule applies.
wired	Clears a rule used for access over a RoamAbout switch's wired-authentication port.
user-glob	User-glob associated with the rule you are removing.

Default

None.

Mode

Enabled.

Example

The following command removes WebAAA for SSID *research* and userglob *temp*@thiscorp.com*:

```
RBT-8100# clear authentication web ssid research temp*@thiscorp.com
```

Related Commands

- clear authentication admin on page 8-4
- clear authentication console on page 8-5
- clear authentication dot1x on page 8-6
- clear authentication mac on page 8-7
- set authentication web on page 8-38
- show aaa on page 8-62

clear location policy

Removes a rule from the location policy on a RAS.

Syntax

clear location policy *rule-number*

Parameters

rule-number	Index number of a location policy rule to remove from the location policy.

Default

None.

Mode

Enabled.

Usage

To determine the index numbers of location policy rules, use the **show location policy** command. Removing all the ACEs from the location policy disables this function on the RAS.

Example

The following command removes location policy rule 4 from a RAS's location policy:

```
RBT-8100# clear location policy 4
success: clause 4 is removed.
```

Related Commands

- set location policy on page 8-40
- show location policy on page 8-68

clear mac-user

Removes a user profile from the local database on the RAS, for a user who is authenticated by a MAC address.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear mac-user *mac-addr*

Parameters

mac-addr	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

Default

None.

Mode

Enabled.

Usage

Deleting a MAC user's profile from the database deletes the assignment of any attributes in the profile to the user.

Example

The following command removes the user profile for a user at MAC address 01:02:03:04:05:06:

```
RBT-8100# clear mac-user 01:02:03:04:05:06
success: change accepted.
```

Related Commands

- set mac-usergroup attr on page 8-50
- set mac-user attr on page 8-44
- show aaa on page 8-62

clear mac-user attr

Removes an authorization attribute from the user profile in the local database on the RAS, for a user who is authenticated by a MAC address.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear mac-user *mac-addr* **attr** *attribute-name*

Parameters

mac-addr	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
attribute-name	Name of an attribute used to authorize the MAC user for a particular service or session characteristic. (For a list of authorization attributes, see Table 8-1 on page 8-45.)

Default

None.

Mode

Enabled.

Example

The following command removes an access control list (ACL) from the profile of a user at MAC address 01:02:03:04:05:06:

```
RBT-8100# clear mac-user 01:02:03:04:05:06 attr filter-id
success: change accepted.
```

Related Commands

- set mac-user attr on page 8-44
- show aaa on page 8-62

clear mac-user group

Removes a user profile from a MAC user group in the local database on the RAS, for a user who is authenticated by a MAC address.

(To remove a MAC user group profile in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear mac-user *mac-addr* **group**

Parameters

mac-addr	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

Default

None.

Mode

Enabled.

Usage

Removing a MAC user from a MAC user group removes the group name from the user's profile, but does not delete the user group from the local RAS database. To remove the group, use **clear mac-usergroup**.

Example

The following command deletes the user profile for a user at MAC address 01:02:03:04:05:06 from its user group:

```
RBT-8100# clear mac-user 01:02:03:04:05:06 group
success: change accepted.
```

Related Commands

- clear mac-usergroup on page 8-14
- set mac-user on page 8-43
- show aaa on page 8-62

clear mac-usergroup

Removes a user group from the local database on the RAS, for a group of users who are authenticated by a MAC address.

(To delete a MAC user group in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear mac-usergroup *group-name*

Parameters

group-name	Name of an existing MAC user group.

Default

None.

Mode

Enabled.

Usage

To remove a user from a MAC user group, use the **clear mac-user group** command.

Example

The following command deletes the MAC user group *eastcoasters* from the local database:

```
RBT-8100# clear mac-usergroup eastcoasters
success: change accepted.
```

Related Commands

- clear mac-usergroup attr on page 8-15
- set mac-usergroup attr on page 8-50
- show aaa on page 8-62

clear mac-usergroup attr

Removes an authorization attribute from a MAC user group in the local database on the RAS, for a group of users who are authenticated by a MAC address.

(To unconfigure an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear mac-usergroup *group-name* **attr** *attribute-name*

Parameters

group-name	Name of an existing MAC user group.
attribute-name	Name of an attribute used to authorize the MAC users in the user group for a particular service or session characteristic. (For a list of authorization attributes, see Table 8-1 on page 8-45.)

Default

None.

Mode

Enabled.

Usage

To remove the group itself, use the **clear mac-usergroup** command.

Example

The following command removes the members of the MAC user group *eastcoasters* from a VLAN assignment by deleting the VLAN-Name attribute from the group:

```
RBT-8100# clear mac-usergroup eastcoasters attr vlan-name
success: change accepted.
```

Related Commands

- clear mac-usergroup on page 8-14
- set mac-usergroup attr on page 8-50
- show aaa on page 8-62

clear mobility-profile

Removes a Mobility Profile entirely.

Syntax

clear mobility-profile *name*

Parameters

name	Name of an existing Mobility Profile.

Default

None.

Mode

Enabled.

Example

The following command removes the Mobility Profile for user Nin:

```
RBT-8100# clear mobility-profile Nin
success: change accepted.
```

Related Commands

- set mobility-profile on page 8-52
- set mobility-profile mode on page 8-54
- show mobility-profile on page 8-69

clear user

Removes a user profile from the local database on the RAS, for a user with a password.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear user *username*

Parameters

username	Username of a user with a password.

Default

None.

Mode

Enabled.

Usage

Deleting the user's profile from the database deletes the assignment of any attributes in the profile to the user.

Example

The following command deletes the user profile for user Nin:

```
RBT-8100# clear user Nin
success: change accepted.
```

Related Commands

- set user on page 8-55
- show aaa on page 8-62

clear user attr

Removes an authorization attribute from the user profile in the local database on the RAS, for a user with a password.

(To remove an authorization attribute from a RADIUS user profile, see the documentation for your RADIUS server.)

Syntax

clear user *username* **attr** *attribute-name*

Parameters

username	Username of a user with a password.
attribute-name	Name of an attribute used to authorize the user for a particular service or session characteristic. (For a list of authorization attributes, see Table 8-1 on page 45.)

Default

None.

Mode

Enabled.

Example

The following command removes the Session-Timeout attribute from Hosni's user profile:

```
RBT-8100# clear user Hosni attr session-timeout
success: change accepted.
```

Related Commands

- set user attr on page 8-57
- show aaa on page 8-62

clear user group

Removes a user with a password from membership in a user group in the local database on the RAS.

(To remove a user from a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear user *username* **group**

Parameters

username	Username of a user with a password.

Default

None.

Mode

Enabled.

Usage

Removing the user from the group removes the group name from the user's profile, but does not delete either the user or the user group from the local RAS database. To remove the group, use **clear usergroup**.

Example

The following command removes the user Nin from from the user group Nin is in:

```
RBT-8100# clear user Nin group
success: change accepted.
```

Related Commands

- clear usergroup on page 8-20
- set user group on page 8-58
- show aaa on page 8-62

clear usergroup

Removes a user group and its attributes from the local database on the RAS, for users with passwords.

(To delete a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear usergroup *group-name*

Parameters

group-name	Name of an existing user group.

Default

None.

Mode

Enabled.

Usage

Removing a user group from the local RAS database does not remove the user profiles of the group's members from the database.

Example

The following command deletes the *cardiology* user group from the local database:

```
RBT-8100# clear usergroup cardiology
success: change accepted.
```

Related Commands

- clear usergroup attr on page 8-21
- set usergroup on page 8-59
- show aaa on page 8-62

clear usergroup attr

Removes an authorization attribute from a user group in the local database on the RAS.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax

clear usergroup *group-name* **attr** *attribute-name*

Parameters

group-name	Name of an existing user group.
attribute-name	Name of an attribute used to authorize all the users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 8-1 on page 8-45.)

Default

None.

Mode

Enabled.

Example

The following command removes the members of the user group *cardiology* from a network access time restriction by deleting the Time-Of-Day attribute from the group:

```
RBT-8100# clear usergroup cardiology attr time-of-day
success: change accepted.
```

Related Commands

- clear usergroup on page 8-20
- set usergroup on page 8-59
- show aaa on page 8-62

set accounting {admin | console}

Sets up accounting services for specified wireless users with administrative access, and defines the accounting records and where they are sent.

Syntax

set accounting {**admin** | **console**} {*user-glob*} {**start-stop** | **stop-only**} *method1* [*method2*] [*method3*] [*method4*]

Parameters

admin	Users with administrative access to the RAS through Telnet or Web View.
console	Users with administrative access to the RAS through a console connection.
user-glob	Single user or set of users with administrative access or network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.) **Note:** This option does not apply if **mac** is specified. For **mac**, specify a *mac-addr-glob*. (See "MAC Address Globs" on page 1-4.)
start-stop	Sends accounting records at the start and end of a network session.
stop-only	Sends accounting records only at the end of a network session.
method1 *method2* *method3* *method4*	At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on. A method can be one of the following: • **local**—Stores accounting records in the local database on the RAS . When the local accounting storage space is full, MSS overwrites older records with new ones. • *server-group-name*—Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Default

Accounting is disabled for all users by default.

Mode

Enabled.

Usage

For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

Example

The following command issues start-and-stop accounting records at the local RAS database for administrator Natasha, when she accesses the switch using Telnet or Web View:

```
RBT-8100# set accounting admin Natasha start-stop local
success: change accepted.
```

Related Commands

- clear accounting on page 8-3
- show accounting statistics on page 8-65

set accounting {dot1x | mac | web | last-resort}

Sets up accounting services for specified wireless users with network access, and defines the accounting records and where they are sent.

Syntax

```
set accounting {dot1x | mac | web} {ssid ssid-name | wired} {user-glob |
mac-addr-glob} {start-stop | stop-only} method1 [method2] [method3] [method4]
```

Parameters

dot1x	Users with network access through the RoamAbout Switch who are authenticated by 802.1X.
mac	Users with network access through the RoamAbout Switch who are authenticated by MAC authentication.
web	Users with network access through the RoamAbout Switch who are authenticated by WebAAA.
last-resort	Users with network access through the RoamAbout Switch who are authenticated with limited access.
ssid ssid-name	SSID name to which this accounting rule applies. To apply the rule to all SSIDs, type **any**.
wired	Applies this accounting rule specifically to users who are authenticated on a wired authentication port.
user-glob	Single user or set of users with administrative access or network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.) **Note:** This option does not apply if **mac** or **last-resort** is specified. For **mac**, specify a *mac-addr-glob*.
mac-addr-glob	A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 1-4.) This option applies only when **mac** is specified.
start-stop	Sends accounting records at the start and end of a network session.
stop-only	Sends accounting records only at the end of a network session.

method1 *method2* *method3* *method4*	At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on. A method can be one of the following: • **local**—Stores accounting records in the local database on the RAS . When the local accounting storage space is full, MSS overwrites older records with new ones. • *server-group-name*—Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Default

Accounting is disabled for all users by default.

Mode

Enabled.

Usage

For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

Example

The following command issues stop-only records to the RADIUS server group *sg2* for network user Nin, who is authenticated by 802.1X:

```
RBT-8100# set accounting dot1x Nin stop-only sg2
success: change accepted.
```

Related Commands

- clear accounting on page 8-3
- show accounting statistics on page 8-65

set accounting system

Configures MSS to send Accounting-On and Accounting-Off messages to a specified RADIUS server group.

Syntax

set accounting system *method1* [*method2*] [*method3*] [*method4*]

Parameters

method1 *method2* *method3* *method4*	At least one of up to four methods that MSS uses to process accounting records. Specify one or more methods in priority order. If the first method does not succeed, MSS tries the second method, and so on. **Note:** The **local** method is not valid for this command.

Default

By default MSS does not send Accounting-On or Accounting-Off messages.

Mode

Enabled.

Usage

Use this command to configure MSS to send an Accounting-On message (Acct-Status-Type = 7) to a RADIUS server when the RoamAbout Switch starts, and an Accounting-Off message (Acct-Status-Type = 8) to the RADIUS server when the RoamAbout Switch is adminstratively shut down.

When you enable this command, an Accounting-On message is generated and sent to the specified server or server group. Subsequent Accounting-On messages are generated each time the RoamAbout Switch starts. When the RoamAbout Switch is administratively shut down, an Accounting-Off message is generated.

Accounting-Off messages are sent only when the RoamAbout Switch is administratively shut down, not when a critical failure causes the RoamAbout Switch to reset. The RoamAbout Switch does not wait for a RADIUS server to acknowledge the Accounting-Off message; the switch makes one attempt to send the Accounting-Off message, then shuts down.

Example

The following command causes Accounting-On and Accounting-Off messages to be sent to RADIUS server group *shorebirds*:

```
RBT-8100# set accounting system shorebirds
success: change accepted.
```

Related Commands

clear accounting on page 8-3

show accounting statistics on page 8-65

set authentication admin

Configures authentication and defines where it is performed for specified users with administrative access through Telnet or Web View.

Syntax

set authentication admin *user-glob method1* [*method2*] [*method3*] [*method4*]

Parameters

user-glob	Single user or set of users with administrative access over the network through Telnet or Web View. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
method1 *method2* *method3* *method4*	At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them. A method can be one of the following: • **local**—Uses the local database of usernames and user groups on the RAS for authentication. • *server-group-name*—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. • **none**—*For users with administrative access only,* MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks. **Note:** The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the RoamAbout switch by an administrator. The fallthru authentication type **none** denies access to a network user. (See "set service-profile auth-fallthru" on page 11-82.) For more information, see "Usage."

Default

By default, authentication is deactivated for all admin users. The default authentication method in an admin authentication rule is **local**. MSS checks the local RAS database for authentication.

Mode

Enabled.

Note: The syntax descriptions for the **set authentication** commands have been separated for clarity. However, the options and behavior for the **set authentication admin** command are the same as in previous releases.

Usage

You can configure different authentication methods for different groups of users. (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 1-3.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local RAS database and sends an authentication request to the RADIUS server group.

Note: If a AAA rule specifies local as a secondary AAA method, to be used if the RADIUS servers are unavailable, and MSS authenticates a client with the local method, MSS starts again at the beginning of the method list when attempting to authorize the client. This can cause unexpected delays during client processing and can cause the client to time out before completing logon.

Example

The following command configures administrator Jose, who connects via Telnet, for authentication on RADIUS server group *sg3*:

```
RBT-8100# set authentication admin Jose sg3
success: change accepted.
```

Related Commands

- clear authentication admin on page 8-4
- set authentication console on page 8-29
- set authentication dot1x on page 8-31
- set authentication mac on page 8-35
- set authentication web on page 8-38
- show aaa on page 8-62

set authentication console

Configures authentication and defines where it is performed for specified users with administrative access through a console connection.

Syntax

set authentication console *user-glob method1* [*method2*] [*method3*] [*method4*]

Parameters

user-glob	Single user or set of users with administrative access through the switch's console. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
method1 *method2* *method3* *method4*	At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them. A method can be one of the following: • **local**—Uses the local database of usernames and user groups on the RAS for authentication. • *server-group-name*—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. • **none**—*For users with administrative access only,* MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks. **Note:** The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the RoamAbout switch by an administrator. The fallthru authentication type **none** denies access to a network user. (See "set service-profile auth-fallthru" on page 11-82.) For more information, see "Usage."

Default

By default, authentication is deactivated for all console users, and the default authentication method in a console authentication rule is **none**. MSS requires no username or password, by default. These users can press Enter at the prompts for administrative access.

Note: Enterasys Networks recommends that you change the default setting unless the RoamAbout switch is in a secure physical location.

Mode

Enabled.

Note: The syntax descriptions for the **set authentication** commands have been separated for clarity. However, the options and behavior for the **set authentication console** command are the same as in previous releases.

Usage

You can configure different authentication methods for different groups of users. (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 1-3.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local RAS database and sends an authentication request to the RADIUS server group.

Example

To set the console port so that it does *not* enforce username-password authentication for administrators, type the following command:

```
RBT-8100# set authentication console * none
success: change accepted.
```

Related Commands

- clear authentication console on page 8-5
- set authentication admin on page 8-27
- set authentication dot1x on page 8-31
- set authentication mac on page 8-35
- set authentication web on page 8-38
- show aaa on page 8-62

set authentication dot1x

Configures authentication and defines how and where it is performed for specified wireless or wired authentication clients who use an IEEE 802.1X authentication protocol to access the network through the RAS.

Syntax

set authentication dot1x {**ssid** *ssid-name* | **wired**} *user-glob* [**bonded**] *protocol method1* [*method2*] [*method3*] [*method4*]

Parameters

ssid ssid-name	SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
wired	Applies this authentication rule specifically to users connected to a wired authentication port.
user-glob	A single user or a set of users with 802.1X network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
bonded	Enables Bonded Auth™ (bonded authentication). When this feature is enabled, MSS authenticates the user only if the machine the user is on has already been authenticated.

protocol	Protocol used for authentication. Specify one of the following: • **eap-md5**—Extensible Authentication Protocol (EAP) with message-digest algorithm 5. *For wired authentication clients*: – Uses challenge-response to compare hashes – Provides *no* encryption or integrity checking for the connection **Note:** The **eap-md5** option does not work with Microsoft wired authentication clients. • **eap-tls**—EAP with Transport Layer Security (TLS): – Provides mutual authentication, integrity-protected negotiation, and key exchange – Requires X.509 public key certificates on both sides of the connection – Provides encryption and integrity checking for the connection – Cannot be used with RADIUS server authentication (requires user information to be in the switch's local database) • **peap-mschapv2**—Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP-V2). *For wireless clients*: – Uses TLS for encryption and data integrity checking and server-side authentication – Provides MS-CHAP-V2 mutual authentication – Only the server side of the connection needs a certificate. The wireless client authenticates using TLS to set up an encrypted session. Then MS-CHAP-V2 performs mutual authentication using the specified AAA method. • **pass-through**—MSS sends all the EAP protocol processing to a RADIUS server.
method1 *method2* *method3* *method4*	At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them. A method can be one of the following: • **local**—Uses the local database of usernames and user groups on the RAS for authentication. • *server-group-name*—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. RADIUS servers cannot be used with the EAP-TLS protocol. For more information, see "Usage."

Default

By default, authentication is unconfigured for all clients with network access through AP ports or wired authentication ports on the RAS. Connection, authorization, and accounting are also disabled for these users.

Bonded authentication is disabled by default.

Mode

Enabled.

Usage

You can configure different authentication methods for different groups of users by "globbing." (For details, see "User Globs" on page 1-3.)

You can configure a rule either for wireless access to an SSID, or for wired access through a RoamAbout switch's wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

You cannot configure client authentication that uses both the EAP-TLS protocol and one or more RADIUS servers. EAP-TLS authentication is supported only on the local RAS database.

If you specify multiple authentication methods in the **set authentication dot1x** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local RAS database and sends an authentication request to the server group.

If the user does not support 802.1X, MSS attempts to perform MAC authentication for the user. In this case, if the switch's configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user's MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **web-portal** (for WebAAA), or **none**.

Example

The following command configures EAP-TLS authentication in the local RAS database for SSID *mycorp* and 802.1X client Geetha:

```
RBT-8100# set authentication dot1x ssid mycorp Geetha eap-tls local
success: change accepted.
```

The following command configures PEAP-MS-CHAP-V2 authentication at RADIUS server groups *sg1* through *sg3* for all 802.1X clients at *example.com* who want to access SSID *examplecorp*:

```
RBT-8100# set authentication dot1x ssid examplecorp *@example.com peap-mschapv2
sg1 sg2 sg3
success: change accepted.
```

Related Commands

- clear authentication dot1x on page 8-6
- set authentication admin on page 8-27
- set authentication console on page 8-29
- set authentication mac on page 8-35
- set authentication web on page 8-38
- set service-profile auth-fallthru on page 11-82
- show aaa on page 8-62

set authentication mac

Configures authentication and defines where it is performed for specified non-802.1X users with network access through a media access control (MAC) address.

Syntax

set authentication mac {**ssid** *ssid-name* | **wired**} *mac-addr-glob method1* [*method2*] [*method3*] [*method4*]

Parameters

ssid *ssid-name*	SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
wired	Applies this authentication rule specifically to users connected to a wired authentication port.
mac-addr-glob	A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 1-4.)
method1 *method2* *method3* *method4*	At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them. A method can be one of the following: • **local**—Uses the local database of usernames and user groups on the RAS for authentication. • *server-group-name*—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. For more information, see "Usage."

Default

By default, authentication is deactivated for all MAC users, which means MAC address authentication fails by default. When using RADIUS for authentication, the default well-known password for MAC and last-resort users is **nopassword**.

Mode

Enabled.

Usage

You can configure different authentication methods for different groups of MAC addresses by "globbing." (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 1-3.)

If you specify multiple authentication methods in the **set authentication mac** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.

- However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local RAS database and sends an authentication request to the RADIUS server group.

If the switch's configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user's MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **w**eb-portal (for WebAAA), or **none**.

Example

To use the local RAS database to authenticate all users who access the *mycorp2* SSID by their MAC address, type the following command:

```
RBT-8100# set authentication ssid mycorp2 mac ** local
success: change accepted.
```

Related Commands

- clear authentication mac on page 8-7
- set authentication admin on page 8-27
- set authentication console on page 8-29
- set authentication dot1x on page 8-31
- set authentication web on page 8-38
- show aaa on page 8-62

set authentication proxy

Configures a proxy authentication rule for a third-party AP's wireless users.

Syntax

set authentication proxy ssid *ssid-name user-glob radius-server-group*

Parameters

ssid *ssid-name*	SSID name to which this authentication rule applies.
user-glob	A single user or a set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
radius-server-group	A group of RADIUS servers used for authentication.

Default

None.

Mode

Enabled.

Usage

AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the *RoamAbout Mobility System Software Configuration Guide*.

Example

The following command configures a proxy authentication rule that matches on all usernames associated with SSID *mycorp*. MSS uses RADIUS server group *srvrgrp1* to proxy RADIUS requests and hence to authenticate and authorize the users.

```
RBT-8100# set authentication proxy ssid mycorp ** srvrgrp1
```

Related Commands

- clear authentication proxy on page 8-8
- set radius proxy client on page 16-12
- clear radius proxy port on page 16-6

set authentication web

Configures an authentication rule to allow a user to log in to the network using a web page served by the RoamAbout switch. The rule can be activated if the user is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

Syntax

set authentication web {**ssid** *ssid-name* | **wired**} *user-glob method1* [*method2*] [*method3*] [*method4*]

Parameters

user-glob	A single user or a set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
ssid ssid-name	SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
wired	Applies this authentication rule specifically to users connected to a wired authentication port.
method1 *method2* *method3* *method4*	At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them. A method can be one of the following: • **local**—Uses the local database of usernames and user groups on the RAS for authentication. • *server-group-name*—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. RADIUS servers cannot be used with the EAP-TLS protocol. For more information, see "Usage."

Default

By default, authentication is unconfigured for all clients with network access through AP ports or wired authentication ports on the RAS. Connection, authorization, and accounting are also disabled for these users.

Mode

Enabled.

Usage

You can configure different authentication methods for different groups of users by "globbing." (For details, see "User Globs" on page 1-3.)

You can configure a rule either for wireless access to an SSID, or for wired access through a RoamAbout switch's wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

If you specify multiple authentication methods in the **set authentication web** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local RAS database and sends an authentication request to the server group.

MSS uses a WebAAA rule only under the following conditions:

- The client is not denied access by 802.1X or does not support 802.1X.
- The client's MAC address does not match a MAC authentication rule.
- The fallthru type is **web**. (For a wireless authentication rule, the fallthru type is specified by the **set service-profile auth-fallthru** command. For a wired authentication rule, the fallthru type is specified by the **auth-fall-thru** option of the **set port type wired-auth** command.)

Example

The following command configures a WebAAA rule in the local RAS database for SSID *ourcorp* and userglob *rnd**:

```
RBT-8100# set authentication web ssid ourcorp rnd* local
success: change accepted.
```

Related Commands

- clear authentication web on page 8-9
- set authentication admin on page 8-27
- set authentication console on page 8-29
- set authentication dot1x on page 8-31
- show aaa on page 8-62

set location policy

Creates and enables a location policy on a RAS. A location policy enables you to locally set or change authorization attributes for a user after the user is authorized by AAA, without making changes to the AAA server.

Syntax

```
set location policy deny if {ssid operator ssid-name | vlan operator vlan-glob |
user operator user-glob | port port-list | dap dap-num} [before rule-number |
modify rule-number]
```

Syntax

```
set location policy permit {vlan vlan-name | inacl inacl-name | outacl
outacl-name} if {ssid operator ssid-name | vlan operator vlan-glob |
user operator user-glob | port port-list | dap dap-num} [before rule-number |
modify rule-number]
```

ParametersI

deny	Denies access to the network to users with characteristics that match the location policy rule.
permit	Allows access to the network or to a specified VLAN, and/or assigns a particular security ACL to users with characteristics that match the location policy rule.
Action options—For a permit rule, MSS changes the attributes assigned to the user to the values specified by the following options:	
vlan *vlan-name*	Name of an existing VLAN to assign to users with characteristics that match the location policy rule.
inacl *inacl-name*	Name of an existing security ACL to apply to packets *sent to* the RAS with characteristics that match the location policy rule. Optionally, you can add the suffix **.in** to the name.
outacl *outacl-name*	Name of an existing security ACL to apply to packets *sent from* the RAS with characteristics that match the location policy rule. Optionally, you can add the suffix **.out** to the name.
Condition options—MSS takes the action specified by the rule if all conditions in the rule are met. You can specify one or more of the following conditions:	
ssid *operator ssid-name*	SSID with which the user is associated. The *operator* must be **eq**, which applies the location policy rule to all users associated with the SSID. Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.

vlan *operator vlan-glob*	VLAN-Name attribute assigned by AAA and condition by which to determine if the location policy rule applies. Replace *operator* with one of the following operands: • **eq**—Applies the location policy rule to all users assigned VLAN names matching *vlan-glob.* • **neq**—Applies the location policy rule to all users assigned VLAN names *not* matching *vlan-glob.* For *vlan-glob*, specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "VLAN Globs" on page 1-4.)
user *operator user-glob*	Username and condition by which to determine if the location policy rule applies. Replace *operator* with one of the following operands: • **eq**—Applies the location policy rule to all usernames matching *user-glob.* • **neq**—Applies the location policy rule to all usernames *not* matching *user-glob.* For *user-glob*, specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
before *rule-number*	Inserts the new location policy rule in front of another rule in the location policy. Specify the number of the existing location policy rule. (To determine the number, use the **show location policy** command.)
modify *rule-number*	Replaces the rule in the location policy with the new rule. Specify the number of the existing location policy rule. (To determine the number, use the **show location policy** command.)
port *port-list*	List of physical port(s) by which to determine if the location policy rule applies.

By default, users are permitted VLAN access and assigned security ACLs according to the VLAN-Name and Filter-Id attributes applied to the users during normal authentication and authorization.

Mode

Enabled.

Usage

Only a single location policy is allowed per RAS. Once configured, the location policy becomes effective immediately. To disable location policy operation, use the **clear location policy** command.

Conditions within a rule are ANDed. All conditions in the rule must match in order for MSS to take the specified action. If the location policy contains multiple rules, MSS compares the user information to the rules one at a time, in the order the rules appear in the switch's configuration file, beginning with the rule at the top of the list. MSS continues comparing until a user matches all conditions in a rule or until there are no more rules.

The order of rules in the location policy is important to ensure users are properly granted or denied access. To position rules within the location policy, use **before** *rule-number* and **modify** *rule-number* in the **set location policy** command, and the **clear location policy** *rule-number* command.

When applying security ACLs:

- Use **inacl** *inacl-name* to filter traffic that enters the switch from users via an AP access port or wired authentication port, or from the network via a network port.
- Use **outacl** *outacl-name* to filter traffic sent from the switch to users via an AP access port or wired authentication port, or from the network via a network port.
- You can optionally add the suffixes **.in** and **.out** to *inacl-name* and *outacl-name* so that they match the names of security ACLs stored in the local RAS database.

Example

The following command denies network access to all users at *.theirfirm.com, causing them to fail authorization:

```
RBT-8100# set location policy deny if user eq *.theirfirm.com
```

The following command authorizes access to the *guest_1* VLAN for all users who are not at *.wodefirm.com:

```
RBT-8100# set location policy permit vlan guest_1 if user neq *.wodefirm.com
```

The following command authorizes users at *.ny.ourfirm.com to access the *bld4.tac* VLAN instead, and applies the security ACL *tac_24* to the traffic they receive:

```
RBT-8100# set location policy permit vlan bld4.tac outacl tac_24 if user eq
*.ny.ourfirm.com
```

The following command authorizes access to users on VLANs with names matching *bld4.** and applies security ACLs *svcs_2* to the traffic they send and *svcs_3* to the traffic they receive:

```
RBT-8100# set location policy permit inacl svcs_2 outacl svcs_3 if vlan eq
bldg4.*
```

The following command authorizes users entering the network on RAS ports 3 through 7 and port 12 to use the *floor2* VLAN, overriding any settings from AAA:

```
RBT-8100# set location policy permit vlan floor2 if port 3-7,12
```

The following command places all users who are authorized for SSID *tempvendor_a* into VLAN *kiosk_1*:

```
RBT-8100# set location policy permit vlan kiosk_1 if ssid eq tempvendor_a
success: change accepted.
```

Related Commands

- clear location policy on page 8-10
- show location policy on page 8-68

set mac-user

Configures a user profile in the local database on the RAS for a user who can be authenticated by a MAC address, and optionally adds the user to a MAC user group.

(To configure a MAC user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax

set mac-user *mac-addr* [**group** *group-name*]

mac-addr	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
group-name	Name of an existing MAC user group.

Default

None.

Mode

Enabled.

Usage

MSS does not require MAC users to belong to user groups.

Users authenticated by MAC address can be authenticated only for network access through the RAS. MSS does not support passwords for MAC users.

Example

The following command creates a user profile for a user at MAC address 01:02:03:04:05:06 and assigns the user to the *eastcoasters* user group:

```
RBT-8100# set mac-user 01:02:03:04:05:06 group eastcoasters
success: change accepted.
```

Related Commands

- clear mac-user on page 8-11
- show aaa on page 8-62

set mac-user attr

Assigns an authorization attribute in the local database on the RAS to a user who is authenticated by a MAC address.

(To assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax

set mac-user *mac-addr* **attr** *attribute-name value*

Parameters

mac-addr	MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
attribute-name value	Name and value of an attribute you are using to authorize the MAC user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to local users, see Table 8-1 on page 8-45.

Default

None.

Mode

Enabled.

Usage

To change the value of an attribute, enter **set mac-user attr** with the new value. To delete an attribute, use **clear mac-user attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

Table 8-1 Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
encryption-type	Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected. **Note:** Encryption-Type is an Enterasys Networks vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 3.	One of the following numbers that identifies an encryption algorithm: • **1**—AES_CCM (Advanced Encryption Standard using Counter with CBC-MAC) • **2**—Reserved • **4**—TKIP (Temporal Key Integrity Protocol) • **8**—WEP_104 (the default) (Wired-Equivalent Privacy protocol using 104 bits of key strength) • **16**—WEP_40 (Wired-Equivalent Privacy protocol using 40 bits of key strength) • **32**—NONE (no encryption) • **64**—Static WEP In addition to these values, you can specify a sum of them for a combination of allowed encryption types. For example, to specify WEP_104 and WEP_40, use **24**.
end-date	Date and time after which the user is no longer allowed to be on the network.	Date and time, in the following format: YY/MM/DD-HH:MM You can use **end-date** alone or with **start-date**. You also can use **start-date**, **end-date**, or both in conjunction with **time-of-day**.
filter-id (network access mode only)	Security access control list (ACL), to permit or deny traffic received (input) or sent (output) by the RAS. (For more information about security ACLs, see Chapter 14, **Security ACL Commands**.)	Name of an existing security ACL, up to 253 alphanumeric characters, with no tabs or spaces. • Use *acl-name***.in** to filter traffic that enters the switch *from users* via an AP access port or wired authentication port, or from the network via a network port. • Use *acl-name***.out** to filter traffic sent from the switch *to users* via an AP access port or wired authentication port, or from the network via a network port. **Note:** If the Filter-Id value returned through the authentication and authorization process does not match the name of a committed security ACL in the RoamAbout switch, the user fails authorization and is unable to authenticate.
idle-timeout	This option is not implemented in the current MSS version.	

Table 8-1 Authentication Attributes for Local Users (continued)

Attribute	Description	Valid Value(s)
mobility-profile (network access mode only)	Mobility Profile attribute for the user. (For more information, see **set mobility-profile** on page 8-52.) **Note:** Mobility-Profile is an Enterasys Networks vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 2.	Name of an existing Mobility Profile, which can be up to 32 alphanumeric characters, with no tabs or spaces. **Note:** If the Mobility Profile feature is enabled, and a user is assigned the name of a Mobility Profile that does not exist on the RoamAbout switch, the user is denied access.
service-type	Type of access the user is requesting.	One of the following numbers: • **2**—Framed; for network user access • **6**—Administrative; for administrative access to the RoamAbout switch, with authorization to access the enabled (configuration) mode. The user must enter the **enable** command and the correct enable password to access the enabled mode. • **7**—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the user can still enter the **enable** command and the correct enable password to access the enabled mode. For administrative sessions, the RoamAbout switch always sends 6 (Administrative). The RADIUS server can reply with one of the values listed above. If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access.
session-timeout (network access mode only)	Maximum number of seconds for the user's session.	Number between 0 and 4,294,967,296 seconds (approximately 136.2 years). **Note:** If the global reauthentication timeout (set by the **set dot1x reauth-period** command) is shorter than the session-timeout, MSS uses the global timeout instead.
ssid (network access mode only)	SSID the user is allowed to access after authentication.	Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to Enterasys Networks radios in the Mobility Domain.

Table 8-1 Authentication Attributes for Local Users (continued)

Attribute	Description	Valid Value(s)
start-date	Date and time at which the user becomes eligible to access the network. MSS does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified).	Date and time, in the following format: YY/MM/DD-HH:MM You can use **start-date** alone or with **end-date**. You also can use **start-date**, **end-date**, or both in conjunction with **time-of-day**.
time-of-day (network access mode only)	Day(s) and time(s) during which the user is permitted to log into the network. After authorization, the user's session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter. **Note:** Time-Of-Day is an Enterasys Networks vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 4.	One of the following: • **never**—Access is always denied. • **any**—Access is always allowed. • **al**—Access is always allowed. • One or more ranges of values that consist of one of the following day designations (required), and a time range in *hhmm-hhmm* 4-digit 24-hour format (optional): – **mo**—Monday – **tu**—Tuesday – **we**—Wednesday – **th**—Thursday – **fr**—Friday – **sa**—Saturday – **su**—Sunday – **wk**—Any day between Monday and Friday Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (|). Do not use spaces. The maximum number of characters is 253. **Note:** You can use **time-of-day** in conjunction with **start-date**, **end-date**, or both.

Table 8-1 Authentication Attributes for Local Users (continued)

Attribute	Description	Valid Value(s)
url (network access mode only)	URL to which the user is redirected after successful WebAAA.	Web URL, in standard format. For example: http://www.example.com **Note:** You must include the *http://* portion. You can dynamically include any of the variables in the URL string: • **$u**—Username • **$v**—VLAN • **$s**—SSID • **$p**—Service profile name To use the literal character $ or ?, use the following: • **$$** • **$q**
vlan-name (network access mode only)	Virtual LAN (VLAN) assignment. **Note:** VLAN-Name is an Enterasys Networks vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 1. **Note:** On some RADIUS servers, you might need to use the standard RADIUS attribute Tunnel-Pvt-Group-ID, instead of VLAN-Name.	Name of a VLAN that you want the user to use. The VLAN must be configured on a RAS within the Mobility Domain to which this RAS belongs.
acct-interim-interval	Interval in seconds between accounting updates, if start-stop accounting mode is enabled.	Number between 180 and 3,600 seconds, or **0** to disable periodic accounting updates. The RoamAbout Switch ignores the acct-interim-interval value and issues a log message if the value is below 60 seconds. If both a RADIUS server and the RoamAbout Switch supply a value for the acct-interim-interval attribute, then the value from the RoamAbout Switch takes precedence.

Example

The following command assigns input access control list (ACL) *acl-03* to filter the packets from a user at MAC address 01:02:03:04:05:06:

```
RBT-8100# set mac-user 01:02:03:04:05:06 attr filter-id acl-03.in
success: change accepted.
```

The following command restricts a user at MAC address 06:05:04:03:02:01 to network access between 7 p.m. on Mondays and Wednesdays and 7 a.m. on Tuesdays and Thursdays:

```
RBT-8100# set mac-user 06:05:04:03:02:01 attr time-of-day mo1900-
1159,tu0000-0700,we1900-1159,th0000-0700
```

```
success: change accepted.
```

Related Commands

- clear mac-user attr on page 8-12
- show aaa on page 8-62

set mac-usergroup attr

Creates a user group in the local database on the RAS for users who are authenticated by a MAC address, and assigns authorization attributes for the group.

(To configure a user group and assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax

set mac-usergroup *group-name* **attr** *attribute-name value*

Parameters

group-name	Name of a MAC user group. Specify a name of up to 32 alphanumeric characters, with no spaces. The name must begin with an alphabetic character.
attribute-name value	Name and value of an attribute you are using to authorize all MAC users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 8-1 on page 8-45.)

Default

None.

Mode

Enabled.

Usage

To change the value of an attribute, enter **set mac-usergroup attr** with the new value. To delete an attribute, use **clear mac-usergroup attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

Example

The following command creates the MAC user group *eastcoasters* and assigns the group members to VLAN *orange*:

```
RBT-8100# set mac-usergroup eastcoasters attr vlan-name orange
success: change accepted.
```

Related Commands

- clear mac-usergroup attr on page 8-15
- show aaa on page 8-62

set mobility-profile

Creates a Mobility Profile and specifies the access point and/or wired authentication ports on the RoamAbout switch through which any user assigned to the profile is allowed access.

Syntax

set mobility-profile name *name* {**port** {**none** | **all** | *port-list*}} | {**dap** {**none** | **all** | *dap-num*}}

Parameters

name	Name of the Mobility Profile. Specify up to 32 alphanumeric characters, with no spaces.
none	Prevents any user to whom this profile is assigned from accessing any access point or wired authentication port on the RoamAbout switch.
all	Allows any user to whom this profile is assigned to access all AP access ports and wired authentication port on the RoamAbout switch.
port-list	List of AP access ports or wired authentication ports through which any user assigned this profile is allowed access. The same port can be used in multiple Mobility Profile port lists.
dap-num	List of Distributed AP connections through which any user assigned this profile is allowed access. The same Distributed AP can be used in multiple Mobility Profile port lists.

Default

No default Mobility Profile exists on the RoamAbout switch. If you do not assign Mobility Profile attributes, all users have access through all ports, unless denied access by other AAA servers or by access control lists (ACLs).

Mode

Enabled.

Usage

To assign a Mobility Profile to a user or group, specify it as an authorization attribute in one of the following commands:

- **set user attr mobility-profile** *name*
- **set usergroup attr mobility-profile** *name*
- **set mac-user attr mobility-profile** *name*
- **set mac-usergroup attr mobility-profile** *name*

To enable the use of the Mobility Profile feature on the RoamAbout switch, use the **set mobility-profile mode** command.

Caution: When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local RoamAbout switch database or RADIUS server when no Mobility Profile of that name exists on the RoamAbout switch.

To change the ports in a profile, use **set mobility-profile** again with the updated port list.

Example

The following commands create the Mobility Profile *magnolia*, which restricts user access to port 12; enable the Mobility Profile feature on the RoamAbout switch; and assign the *magnolia* Mobility Profile to user *Jose*.

```
RBT-8100# set mobility-profile name magnolia port 12
success: change accepted.
RBT-8100# set mobility-profile mode enable
success: change accepted.
RBT-8100# set user Jose attr mobility-profile magnolia
success: change accepted.
```

The following command adds port 13 to the *magnolia* Mobility Profile (which is already assigned to port 12):

```
RBT-8100# set mobility-profile name magnolia port 12-13
success: change accepted.
```

Related Commands

- clear mobility-profile on page 8-16
- set mac-user attr on page 8-44
- set mac-usergroup attr on page 8-50
- set mobility-profile mode on page 8-54
- set user attr on page 8-57
- set usergroup on page 8-59
- show mobility-profile on page 8-69

set mobility-profile mode

Enables or disables the Mobility Profile feature on the RoamAbout switch.

Caution: When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local RoamAbout switch database or RADIUS server when no Mobility Profile of that name exists on the RoamAbout switch.

Syntax

```
set mobility-profile mode {enable | disable}
```

Parameters

enable	Enables the use of the Mobility Profile feature on the RoamAbout switch.
disable	Specifies that all Mobility Profile attributes are ignored by the RoamAbout switch.

Default

The Mobility Profile feature is disabled by default.

Mode

Enabled.

Example

To enable the use of the Mobility Profile feature, type the following command:

```
RBT-8100# set mobility-profile mode enable
success: change accepted.
```

Related Commands

- clear mobility-profile on page 8-16
- set mobility-profile on page 8-52
- show mobility-profile on page 8-69

set user

Configures a user profile in the local database on the RAS for a user with a password.

(To configure a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax

set user *username* **password** [**encrypted**] *string*

Parameters

username	Username of a user with a password.
password *string*	Password of up to 32 alphanumeric characters, with no spaces.
encrypted	Indicates that the password string you entered is already in its encrypted form. If you use this option, MSS does not encrypt the displayed form of the password string, and instead displays the string exactly as you entered it. If you omit this option, MSS does encrypt the displayed form of the string.

Default

None.

Mode

Enabled.

Usage

The **show config** command shows the **encrypted** option with this command, even when you omit the option. The **encrypted** option appears in the configuration because MSS automatically encrypts the password when you create the user (unless you use the **encrypted** option when you enter the password).

Although MSS allows you to configure a user password for the special "last-resort" guest user, the password has no effect. Last-resort users can never access a RAS in administrative mode and never require a password.

The only valid username of the form *last-resort-** is *last-resort-wired*. The *last-resort-wired* user allows last-resort access on a wired authentication port.

Example

The following command creates a user profile for user Nin in the local database, and assigns the password *goody*:

```
RBT-8100# set user Nin password goody
success: User Nin created
```

The following command assigns the password *chey3nne* to the **admin** user:

```
RBT-8100# set user admin password chey3nne
success: User admin created
```

The following command changes Nin's password from *goody* to *29Jan04:*

```
RBT-8100# set user Nin password 29Jan04
```

Related Commands

- clear user on page 8-17
- show aaa on page 8-62

set user attr

Configures an authorization attribute in the local database on the RAS for a user with a password.

(To assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax

set user *username* **attr** *attribute-name value*

Parameters

username	Username of a user with a password.
attribute-name value	Name and value of an attribute you are using to authorize the user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 8-1 on page 8-45.

Default

None.

Mode

Enabled.

Usage

To change the value of an attribute, enter **set user attr** with the new value. To delete an attribute, use **clear user attr**.

Example

The following command assigns user Tamara to VLAN *orange*:

```
RBT-8100# set user Tamara attr vlan-name orange
success: change accepted.
```

The following command assigns Tamara to the Mobility Profile *tulip.*

```
RBT-8100# set user Tamara attr mobility-profile tulip
success: change accepted.
```

Related Commands

- clear user attr on page 8-18
- show aaa on page 8-62

set user group

Adds a user to a user group. The user must have a password and a profile that exists in the local database on the RAS.

(To configure a user in RADIUS, see the documentation for your RADIUS server.)

Syntax

set user *username* **group** *group-name*

Parameters

username	Username of a user with a password.
group-name	Name of an existing user group for password users.

Default

None.

Mode

Enabled.

Usage

MSS does not require users to belong to user groups.

To *create* a user group, user the command **set usergroup**.

Example

The following command adds user Hosni to the *cardiology* user group:

```
RBT-8100# set user Hosni group cardiology
success: change accepted.
```

Related Commands

- clear user group on page 8-19
- show aaa on page 8-62

set usergroup

Creates a user group in the local database on the RAS for users and assigns authorization attributes for the group.

(To create user groups and assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax

set usergroup *group-name* **attr** *attribute-name value*

Parameters

group-name	Name of a group for password users. Specify a name of up to 32 alphanumeric characters, with no spaces. The name must begin with an alphabetic character.
attribute-name value	Name and value of an attribute you are using to authorize all users in the group for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to users, see Table 8-1 on page 8-45.

Default

None.

Mode

Enabled.

Usage

To change the value of an attribute, enter **set usergroup attr** with the new value. To delete an attribute, use **clear usergroup attr**.

To *add* a user to a group, user the command **set user group**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user's network access can begin as soon as the user start-date. The user does not need to wait for the user group's start date.

Example

The following command adds the user group *cardiology* to the local database and assigns all the group members to VLAN *crimson*:

```
RBT-8100# set usergroup cardiology attr vlan-name crimson
success: change accepted.
```

Related Commands

- clear usergroup on page 8-20
- clear usergroup attr on page 8-21
- show aaa on page 8-62

set web-portal

Globally enables or disables WebAAA on a RoamAbout switch.

Syntax

```
set web-portal {enable | disable}
```

Parameters

enable	Enables WebAAA on the switch.
disable	Disables WebAAA on the switch.

Default

Enabled.

Mode

Enabled.

Usage

This command disables or reenables support for WebAAA. However, WebAAA has additional configuration requirements. For information, see the "Configuring AAA for Network Users" chapter in the *RoamAbout Mobility System Software Configuration Guide*.

Example

To disable WebAAA, type the following command:

```
RBT-8100# set web-portal disable
success: change accepted.
```

Related Commands

- clear authentication web on page 8-9
- set service-profile auth-fallthru on page 11-82
- set user on page 8-55

show aaa

Displays all current AAA settings.

Syntax

show aaa

Parameters

None.

Default

None.

Mode

Enabled.

Example

To display all current AAA settings, type the following command:

```
RBT-8100# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)
Radius Servers
Server                  Addr           Ports   T/o Tries Dead State
-------------------------------------------------------------------------
rs-3                198.162.1.1     1821 1813  5    3    0    UP
rs-4                198.168.1.2     1821 1813  77   11   2    UP
rs-5                198.162.1.3     1821 1813  42   23   0    UP
Server groups
   sg1: rs-3
   sg2: rs-4
   sg3: rs-5

Web Portal:
enabled


set authentication admin Jose sg3
set authentication console * none
set authentication mac ssid mycorp * local
set authentication dot1x ssid mycorp Geetha eap-tls
set authentication dot1x ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set authentication dot1x ssid any ** peap-mschapv2 sg1 sg2 sg3
set accounting dot1x Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local
user Nin
Password = 082c6c64060b (encrypted)
```

```
Filter-Id = acl-999.in
Filter-Id = acl-999.out
user last-resort-guestssid
   Vlan-Name = k2
user last-resort-any
   Vlan-Name = foo
mac-user 01:02:03:04:05:06
usergroup eastcoasters
   session-timeout = 99
```

Table 8-2 describes the fields that can appear in **show aaa** output.

Table 8-2 show aaa Output

Output	What it displays...
Default Values	RADIUS default values for all parameters.
authport	UDP port on the RAS for transmission of RADIUS authorization and authentication messages. The default port is 1812.
acctport	UDP port on the RAS for transmission of RADIUS accounting records. The default is port 1813.
timeout	Number of seconds the RAS waits for a RADIUS server to respond before retransmitting. The default is 5 seconds.
acct-timeout	Number of seconds the RAS waits for a RADIUS server to respond to an accounting request before retransmitting. The default is 5 seconds.
retrans	Number of times the RAS retransmits a message before determining a RADIUS server unresponsive. The default is 3 times.
deadtime	Number of minutes the RAS waits after determining a RADIUS server is unresponsive before trying to reconnect with this server. During the dead time, the RADIUS server is ignored by the RoamAbout switch. The default is 0 minutes.
key	Shared secret key, or password, used to authenticate to a RADIUS server. The default is no key.
author-pass	Password used for outbound authentication to a RADIUS server, used in conjunction with a last-resort username. The default is **nopassword**.
Radius Servers	Information about active RADIUS servers.
Server	Name of each RADIUS server currently active.
Addr	IP address of each RADIUS server currently active.
Ports	UDP ports that the RAS uses for authentication messages and for accounting records.
T/o	Setting of timeouts on each RADIUS server currently active.
Tries	Number of retransmissions configured for each RADIUS server currently active. The default is 3 times.
Dead	Length of time until the server is considered responsive again.
State	Current state of each RADIUS server currently active: • UP (operating) • DOWN (unavailable)

Table 8-2 show aaa Output (continued)

Output	What it displays...
Server groups	Names of RADIUS server groups and member servers configured on the RAS.
Web Portal	State of the WebAAA feature: • enabled • disabled
set commands	List of commands used to configure AAA on the RAS.
user and user group profiles	List of user and user group profiles stored in the local database on the RAS.

Related Commands

- set accounting {admin | console} on page 8-22
- set authentication admin on page 8-27
- set authentication console on page 8-29
- set authentication dot1x on page 8-31
- set authentication mac on page 8-35
- set authentication web on page 8-38

show accounting statistics

Displays the AAA accounting records for wireless users. The records are stored in the local database on the RAS.

(To display RADIUS accounting records, see the documentation for your RADIUS server.)

Syntax

show accounting statistics

Parameters

None.

Default

None.

Mode

Enabled.

Example

To display the locally stored accounting records, type the following command:

```
RBT-8100# show accounting statistics
Dec 14 00:39:48
Acct-Status-Type=STOP
Acct-Authentic=0
Acct-Multi-Session-Id=SESS-3-01f82f-520236-24bb1223
Acct-Session-Id=SESS-3-01f82f-520236-24bb1223
User-Name=vineet
AAA_ACCT_SVC_ATTR=2
Acct-Session-Time=551
Event-Timestamp=1134520788
Acct-Output-Octets=3204
Acct-Input-Octets=1691
Acct-Output-Packets=20
Acct-Input-Packets=19
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

Dec 14 00:39:53
Acct-Status-Type=START
Acct-Authentic=0
User-Name=vineet
Acct-Multi-Session-Id=SESS-4-01f82f-520793-bd779517
Acct-Session-Id=SESS-4-01f82f-520793-bd779517
```

```
Event-Timestamp=1134520793
AAA_ACCT_SVC_ATTR=2
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x
```

Table 8-3 describes the fields that can appear in **show accounting statistics** output.

Table 8-3 show accounting statistics Output

Output	What it displays...
Date and time	Date and time of the accounting record.
Acct-Status-Type	Type of accounting record: • START • STOP • UPDATE
Acct-Authentic	Location where the user was authenticated (if authentication took place) for the session: • 1—RADIUS server • 2—Local RAS database
User-Name	Username of a user with a password.
Acct-Multi-Session-Id	Unique accounting ID for multiple related sessions in a log file.
AAA_TTY_ATTR	For sessions conducted through a console or administrative Telnet connection, the Telnet terminal number.
Event-Timestamp	Time (in seconds since January 1, 1970) at which the event was triggered. (See RFC 2869 for more information.)
Acct-Session-Time	Number of seconds that the session has been online.
Acct-Output-Octets	Number of octets the RAS has sent during the session.
Acct-Input-Octets	Number of octets the RAS has received during the session.
Acct-Output-Packets	Number of packets the RAS has sent during the session.
Acct-Input-Packets	Number of packets the RAS has received during the session.
Vlan-Name	Name of the client's VLAN.
Calling-Station-Id	MAC address of the supplicant (client).
Nas-Port-Id	Number of the port and radio on the AP access point through which the session was conducted.
Called-Station-Id	MAC address of the access point through which the client reached the network.

Related Commands

- clear accounting on page 8-3
- set accounting {admin | console} on page 8-22
- show aaa on page 8-62

show location policy

Displays the list of location policy rules that make up the location policy on a RAS.

Syntax

```
show location policy
```

Parameters

None.

Default

None.

Mode

Enabled.

Example

The following command displays the list of location policy rules in the location policy on a RAS:

```
RBT-8100 show location policy
Id Clauses
-----------------------------------------------------------------
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.wodefirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.wodefirm.com
```

Related Commands

- clear location policy on page 8-10
- set location policy on page 8-40

show mobility-profile

Displays the named Mobility Profile. If you do not specify a Mobility Profile name, this command shows all Mobility Profile names and port lists on the RoamAbout switch.

Syntax

show mobility-profile [*name*]

Parameters

name	Name of an existing Mobility Profile.

Default

None.

Mode

Enabled.

Example

The following command displays the Mobility Profile *magnolia*:

```
RBT-8100# show mobility-profile magnolia
Mobility Profiles
Name                 Ports
=========================
magnolia          AP 12
```

Related Commands

- clear mobility-profile on page 8-16
- set mobility-profile on page 8-52

9

Mobility Domain Commands

Use Mobility Domain commands to configure and manage Mobility Domain groups.

A Mobility Domain is a system of RoamAbout switch access points working together to support a roaming user (client). One RoamAbout switch acts as a seed switch, which maintains and distributes a list of IP addresses of the domain members.

Note: Enterasys Networks recommends that you run the same MSS version on all the RoamAbout switches in a Mobility Domain.

This chapter presents Mobility Domain commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear domain security	9-2
clear mobility-domain	9-3
clear mobility-domain member	9-4
set domain security	9-5
set mobility-domain member	9-6
set mobility-domain mode member seed-ip	9-7
set mobility-domain mode seed domain-name	9-8
show mobility-domain config	9-9
show mobility-domain	9-10

clear domain security

Disables RoamAbout Switch to RoamAbout Switch security.

Syntax

```
clear domain security
```

Default

None.

Mode

Enabled.

Usage

This command is equivalent to the **set domain security none** command.

Example

The following command disables RoamAbout Switch to RoamAbout Switch security on an RoamAbout Switch:

```
RBT-8100# clear domain security
success: change accepted.
```

clear mobility-domain

Clears all Mobility Domain configuration and information from a RoamAbout switch, regardless of whether the RoamAbout switch is a seed or a member of a Mobility Domain.

Syntax

clear mobility-domain

Parameters

None.

Default

None.

Mode

Enabled.

Usage

This command has no effect if the RoamAbout switch is not configured as part of a Mobility Domain.

Example

To clear a Mobility Domain from a RoamAbout switch within the domain, type the following command:

```
RBT-8100# clear mobility-domain
success: change accepted.
```

Related Commands

- clear mobility-domain member on page 9-4
- set mobility-domain member on page 9-6
- set mobility-domain mode member seed-ip on page 9-7
- set mobility-domain mode seed domain-name on page 9-8

clear mobility-domain member

On the seed RoamAbout switch, removes the identified member from the Mobility Domain.

Syntax

clear mobility-domain member *ip-addr*

Parameters

ip-addr	IP address of the Mobility Domain member, in dotted decimal notation.

Default

None.

Mode

Enabled.

Usage

This command has no effect if the RoamAbout switch member is not configured as part of a Mobility Domain or the current RoamAbout switch is not the seed.

Example

The following command clears a Mobility Domain member with the IP address 192.168.0.1:

```
RBT-8100# clear mobility-domain member 192.168.0.1
```

Related Commands

set mobility-domain member on page 9-6

set domain security

Enables RoamAbout Switch to RoamAbout Switch security in the RoamAbout Switch's Mobility Domain.

Syntax

set domain security {**none** | **required**}

Parameters

none	RoamAbout Switch to RoamAbout Switch security is disabled.
required	RoamAbout Switch to RoamAbout Switch security is enabled.

Default

The default is **none**. (RoamAbout Switch to RoamAbout Switch security is disabled.)

Mode

Enabled.

Usage

The setting must be the same (**none** or **required**) on all switches, the seed and all members, in the Mobility Domain.

The **set domain security none** command is equivalent to the **clear domain security** command.

Example

The following command enables RoamAbout Switch to RoamAbout Switch security on an RoamAbout switch:

```
RBT-8100# set domain security required
success: change accepted.
```

set mobility-domain member

On the seed RoamAbout switch, adds a member to the list of Mobility Domain members. If the current RoamAbout switch is not configured as a seed, this command is rejected.

Syntax

set mobility-domain member *ip-addr* **key** *hex-bytes*

Parameters

ip-addr	IP address of the Mobility Domain member in dotted decimal notation.
key *hex-bytes*	Fingerprint of the public key to use for RoamAbout switch security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example: 00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff

Default

None.

Mode

Enabled.

Usage

This command must be entered from the seed RoamAbout switch.

Examples

The following commands add three RoamAbout switches with the IP addresses 192.168.1.8, 192.168.1.9, and 192.168.1.10 as members of a Mobility Domain whose seed is the current RoamAbout switch:

```
RBT-8100# set mobility-domain member 192.168.1.8
success: change accepted.
RBT-8100# set mobility-domain member 192.168.1.9
success: change accepted.
RBT-8100# set mobility-domain member 192.168.1.10
success: change accepted.
```

Related Commands

- clear mobility-domain member on page 9-4
- set mobility-domain mode seed domain-name on page 9-8
- show mobility-domain config on page 9-9

set mobility-domain mode member seed-ip

On a nonseed RoamAbout switch, sets the IP address of the seed RoamAbout switch. This command is used on a member RoamAbout switch to configure it as a member. If the RoamAbout switch is currently part of another Mobility Domain or using another seed, this command overwrites that configuration.

Syntax

set mobility-domain mode member seed-ip *ip-addr* **key** *hex-bytes*

Parameters

ip-addr	IP address of the Mobility Domain member, in dotted decimal notation.
key *hex-bytes*	Fingerprint of the public key to use for RoamAbout Switch to RoamAbout Switch security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example: 00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff

Default

None.

Mode

Enabled.

Example

The following command sets the current RoamAbout switch as a nonseed member of the Mobility Domain whose seed has the IP address 192.168.1.8:

```
RBT-8100# set mobility-domain mode member seed-ip 192.168.1.8
mode is: member
seed IP is: 192.168.1.8
```

Related Commands

- clear mobility-domain on page 9-3
- show mobility-domain config on page 9-9

set mobility-domain mode seed domain-name

Creates a Mobility Domain by setting the current RoamAbout switch as the seed device and naming the Mobility Domain.

Syntax

set mobility-domain mode seed domain-name *mob-domain-name*

Parameters

mob-domain-name	Name of the Mobility Domain. Specify between 1 and 32 characters with no spaces.

Default

None.

Mode

Enabled.

Usage

Before you use this command, the current RoamAbout switch must have its IP address set with the set system ip-address command. After you enter this command, all Mobility Domain traffic is sent and received from the specified IP address.

You must explicitly configure *only one* RoamAbout switch per domain as the seed. All other RoamAbout switches in the domain receive their Mobility Domain information from the seed.

Example

The following command creates a Mobility Domain named Pleasanton with the current RoamAbout switch as the seed:

```
RBT-8100# set mobility-domain mode seed domain-name Pleasanton
mode is: seed
domain name is: Pleasanton
```

Related Commands

- clear mobility-domain member on page 9-4
- show mobility-domain on page 9-10

show mobility-domain config

Displays the configuration of the Mobility Domain.

Syntax

```
show mobility-domain config
```

Parameters

None.

Default

None.

Mode

Enabled.

Example

The following command displays the Mobility Domain configuration:

```
RBT-8100# show mobility-domain config
This switch is a member, with seed 192.168.14.6
```

Related Commands

- clear mobility-domain on page 9-3
- set mobility-domain member on page 9-6
- show mobility-domain on page 9-10

show mobility-domain

On the seed RoamAbout switch, displays the Mobility Domain status and members.

Syntax

show mobility-domain

Parameters

None.

Default

None.

Mode

Enabled.

Example

To display Mobility Domain status, type the following command:

```
RBT-8100# show mobility-domain
Mobility Domain name:  Pleasanton
Member              State             Status
---------------     -------------     --------------
192.168.253.11      STATE_UP          MEMBER
192.168.253.12      STATE_DOWN        MEMBER
192.168.253.14      STATE_UP          SEED
```

Table 9-1 describes the fields in the display.

Table 9-1 Output for show mobility-domain

Output	What It Displays...
Mobility Domain name	Name of the Mobility Domain
Member	IP addresses of the seed RoamAbout switch and members in the Mobility Domain
State	State of the RoamAbout switch in the Mobility Domain: STATE_UP STATE_DOWN
Status	Role of the RoamAbout switch in the Mobility Domain: MEMBER SEED

Related Commands

- clear mobility-domain on page 9-3
- set mobility-domain member on page 9-6
- set mobility-domain mode member seed-ip on page 9-7

10

Network Domain Commands

Use Network Domain commands to configure and manage Network Domain groups.

A Network Domain is a group of geographically dispersed Mobility Domains that share information among themselves over a WAN link. This shared information allows a user configured on an RoamAbout Switch in one Mobility Domain to establish connectivity on an RoamAbout Switch in another Mobility Domain elsewhere in the same Network Domain. The RoamAbout Switch forwards the user traffic by creating a VLAN tunnel to an RoamAbout Switch in the remote Mobility Domain.

In a Network Domain, one or more RoamAbout Switches serve as a seed switch. At least one of the Network Domain seeds maintains a connection with each of the member RoamAbout Switches in the Network Domain. The Network Domain seeds share information about the VLANs configured on their members, so that all the Network Domain seeds have a common database of VLAN information.

This chapter presents Network Domain commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear network-domain	10-2
clear network-domain mode	10-3
clear network-domain peer	10-4
clear network-domain seed-ip	10-5
set network-domain mode member seed-ip	10-6
set network-domain peer	10-7
set network-domain mode seed domain-name	10-8
show network-domain	10-9

clear network-domain

Clears all Network Domain configuration and information from an RoamAbout Switch, regardless of whether the RoamAbout Switch is a seed or a member of a Network Domain.

Syntax

clear network-domain

Defaults

None.

Mode

Enabled.

Usage

This command has no effect if the RoamAbout Switch is not configured as part of a Network Domain.

Examples

To clear a Network Domain from an RoamAbout Switch within the domain, type the following command:

```
RBT-8100# clear network-domain
This will clear all network-domain configuration. Would you like to continue? (y/
n) [n] y
success: change accepted.
```

Related Commands

- set network-domain mode member seed-ip on page 10-6
- set network-domain peer on page 10-7
- set network-domain mode seed domain-name on page 10-8

clear network-domain mode

Removes the Network Domain seed or member configuration from the RoamAbout Switch.

Syntax

```
clear network-domain mode {seed | member}
```

Parameters

seed	Clears the Network Domain seed configuration from the RoamAbout Switch.
member	Clears the Network Domain member configuration from the RoamAbout Switch.

Defaults

None.

Mode

Enabled.

Usage

This command has no effect if the RoamAbout Switch is not configured as part of a Network Domain.

Examples

The following command clears the Network Domain member configuration from the RoamAbout Switch:

```
RBT-8100# clear network-domain mode member
success: change accepted.
```

The following command clears the Network Domain seed configuration from the RoamAbout Switch:

```
RBT-8100# clear network-domain mode seed
success: change accepted.
```

Related Commands

- set network-domain mode member seed-ip on page 10-6
- set network-domain mode seed domain-name on page 10-8

clear network-domain peer

Removes the configuration of a Network Domain peer from an RoamAbout Switch configured as a Network Domain seed.

Syntax

clear network-domain peer {*ip-addr* | **all**}

ip-addr	IP address of the Network Domain peer in dotted decimal notation.
all	Clears the Network Domain peer configuration for all peers from the RoamAbout Switch.

Defaults

None.

Mode

Enabled.

Usage

This command has no effect if the RoamAbout Switch is not configured as a Network Domain seed.

Examples

The following command clears the Network Domain peer configuration for peer 192.168.9.254 from the RoamAbout Switch:

```
RBT-8100# clear network-domain peer 192.168.9.254
success: change accepted.
```

The following command clears the Network Domain peer configuration for all peers from the RoamAbout Switch:

```
RBT-8100# clear network-domain peer all
success: change accepted.
```

Related Commands

set network-domain peer on page 10-7

clear network-domain seed-ip

Removes the specified Network Domain seed from the RoamAbout Switch's configuration. When you enter this command, the Network Domain TCP connections between the RoamAbout Switch and the specified Network Domain seed are closed.

Syntax

clear network-domain seed-ip *ip-addr*

Parameters

ip-addr	IP address of the Network Domain seed in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Usage

This command has no effect if the RoamAbout Switch is not configured as part of a Network Domain, or if the RoamAbout Switch is not configured as a member of a Network Domain that uses the specified Network Domain seed.

Examples

The following command removes the Network Domain seed with IP address 192.168.9.254 from the RoamAbout Switch's configuration:

```
RBT-8100# clear network-domain seed-ip 192.168.9.254
success: change accepted.
```

Related Commands

set network-domain mode member seed-ip on page 10-6

set network-domain mode member seed-ip

Sets the IP address of a Network Domain seed. This command is used for configuring an RoamAbout Switch as a member of a Network Domain. You can specify multiple Network Domain seeds and configure one as the primary seed.

Syntax

set network-domain mode member seed-ip *ip-addr* [**affinity** *num*]

Parameters

ip-addr	IP address of the Network Domain seed, in dotted decimal notation.
num	Preference for using the specified Network Domain seed. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults

The default affinity for a Network Domain seed is 5.

Mode

Enabled.

Usage

You can specify multiple Network Domain seeds on the RoamAbout Switch. When the RoamAbout Switch needs to connect to a Network Domain seed, it first attempts to connect to the seed with the highest affinity. If that seed is unavailable, the RBT attempts to connect to the seed with the next-highest affinity. After a connection is made to a non-highest-affinity seed, the RoamAbout Switch then periodically attempts to connect to the highest-affinity seed.

Examples

The following command sets the RoamAbout Switch as a member of the Network Domain whose seed has the IP address 192.168.1.8:

```
RBT-8100# set network-domain mode member seed-ip 192.168.1.8
success: change accepted.
```

The following command sets the RoamAbout Switch as a member of a Network Domain whose seed has the IP address 192.168.9.254 and sets the affinity for that seed to 7. If the RoamAbout Switch specifies other Network Domain seeds, and they are configured with the default affinity of 5, then 192.168.9.254 becomes the primary Network Domain seed for this RoamAbout Switch.

```
RBT-8100# set network-domain mode member seed-ip 192.168.9.254 affinity 7
success: change accepted.
```

Related Commands

- clear network-domain on page 10-2
- show network-domain on page 10-9

set network-domain peer

On a Network Domain seed, configures one or more RoamAbout Switches as redundant Network Domain seeds. The seeds in a Network Domain share information about the VLANs configured on the member devices, so that all the Network Domain seeds have the same database of VLAN information.

Syntax

set network-domain peer *ip-addr*

Parameters

ip-addr	IP address of the Network Domain seed to specify as a peer, in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Usage

This command must be entered on an RoamAbout Switch configured as a Network Domain seed.

Example

The following command sets the RoamAbout Switch with IP address 192.168.9.254 as a peer of this Network Domain seed:

```
RBT-8100# set network-domain peer 192.168.9.254
success: change accepted.
```

Related Commands

- clear network-domain on page 10-2
- show network-domain on page 10-9

set network-domain mode seed domain-name

Creates a Network Domain by setting the current RoamAbout Switch as a seed device and naming the Network Domain.

Syntax

set network-domain mode seed domain-name *net-domain-name*

net-domain-name	Name of the Network Domain. Specify between 1 and 16 characters with no spaces.

Defaults

None.

Mode

Enabled.

Usage

Before you use this command, the current RoamAbout Switch must have its IP address set with the **set system ip-address** command. After you enter this command, Network Domain traffic is sent and received from the specified IP address.

You can configure multiple RoamAbout Switches as Network Domain seeds. If you do this, you must identify them as peers by using the **set network domain peer** command.

Example

The following command creates a Network Domain named California with the current RoamAbout Switch as a seed:

```
RBT-8100# set network-domain mode seed domain-name California
success: change accepted.
```

Related Commands

- clear network-domain on page 10-2
- show network-domain on page 10-9

show network-domain

Displays the status of Network Domain seeds and members.

Syntax

```
show network-domain
```

Defaults

None.

Mode

Enabled.

Examples

To display Network Domain status, type the following command. The output of the command differs based on whether the RoamAbout Switch is a member of a Network Domain or a Network Domain seed.

On an RoamAbout Switch that is a Network Domain member, the following output is displayed:

```
RBT-8100# show network-domain
Member Network Domain name: California
Member              State             Mode       Mobility-Domain
---------------     -------------     ------     ---------------
10.8.107.1          UP                  SEED     default
```

On an RoamAbout Switch that is a Network Domain seed, information is displayed about the Network Domains of which the RoamAbout Switch is a member, as well as Network Domain seeds with which the RoamAbout Switch has a peer relationship. For example:

```
RBT-8100# show network-domain
Network Domain name: California
Peer                State
---------------     -------------
10.8.107.1          UP
Member              State             Mode       Mobility-Domain
---------------     -------------     ------     ---------------
10.1.0.0            DOWN                SEED
Member Network Domain name:
Member              State             Mode       Mobility-Domain
---------------     -------------     ------     ---------------
10.8.107.1          UP                MEMBER     default
10.1.0.0            DOWN                SEED
```

Table 10-1 describes the fields in the display.

Table 10-1 show network-domain Output

Field	Description
Output if RBT is the Network Domain seed:	
Network Domain name	Name of the Network Domain for which the RoamAbout Switch is a seed.
Peer	IP addresses of the other seeds in the Network Domain.
State	State of the connection between the RoamAbout Switch and the peer Network Domain seeds: • UP • DOWN
Member	IP addresses of the seed RoamAbout Switch and members in the Network Domain
State	State of the RoamAbout Switch in the Network Domain: • UP • DOWN
Mode	Role of the RoamAbout Switch in the Network Domain: • MEMBER • SEED
Mobility-Domain	Name of the Mobility Domain of which the RoamAbout Switch is a member.
Output if RBT is a Network Domain member:	
Member Network Domain name	Name of the Network Domain of which the RoamAbout Switch is a member.
Member	IP addresses of the seed RoamAbout Switch and members in the Network Domain
State	State of the RoamAbout Switch in the Network Domain: • UP • DOWN
Mode	Role of the RoamAbout Switch in the Network Domain: • MEMBER • SEED
Mobility-Domain	Name of the Mobility Domain of which the RoamAbout Switch is a member.

Related Commands

- clear network-domain on page 10-2
- set network-domain mode member seed-ip on page 10-6
- set network-domain mode seed domain-name on page 10-8
- set network-domain peer on page 10-7

11

Access Point Commands

Use access point commands to configure and manage access points. Be sure to do the following before using the commands:

- Define the country-specific IEEE 802.11 regulations on the RoamAbout switch. (Refer to set system countrycode on page 3-16.)
- Install the access point and connect it to a port on the RoamAbout switch. (Refer to the *RoamAbout Wireless Switch Installation Guide* specific to your wireless switch.)
- Configure an access point access port for a Distributed access point.

Caution: Changing the system country code after access point configuration disables access points and deletes their configuration. If you change the country code on a RoamAbout switch, you must reconfigure all access points.

This chapter presents access point commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear {ap | dap} radio	11-5
clear dap boot-configuration	11-7
clear radio-profile	11-8
clear service-profile	11-10
reset {ap | dap}	11-12
set dap auto	11-13
set dap auto mode	11-15
set dap auto persistent	11-16
set dap auto radiotype	11-17
set {ap | dap} bias	11-18
set {ap | dap} blink	11-19
set dap boot-ip	11-20
set dap boot-switch	11-22
set dap boot-vlan	11-24
set dap fingerprint	11-26
set {ap | dap} force-image-download	11-27

For information about...	Refer to page...
set {ap | dap} group	11-28
set {ap | dap} image	11-29
set {ap | dap} location	11-29
set {ap | dap} name	11-30
set {ap | dap} radio antenna-location	11-31
set {ap | dap} radio antennatype	11-32
set {ap | dap} radio auto-tune max-power	11-33
set {ap | dap} radio channel	11-35
set {ap | dap} radio auto-tune min-client-rate	11-36
set {ap | dap} radio mode	11-38
set {ap | dap} radio radio-profile	11-39
set {ap | dap} radio tx-power	11-40
set dap security	11-42
set {ap | dap} upgrade-firmware	11-44
set radio-profile active-scan	11-45
set radio-profile auto-tune channel-config	11-46
set radio-profile auto-tune channel-holddown	11-48
set radio-profile auto-tune channel-interval	11-49
set radio-profile auto-tune channel-lockdown	11-49
set radio-profile auto-tune power-config	11-52
set radio-profile auto-tune power-interval	11-53
set radio-profile beacon-interval	11-56
set radio-profile countermeasures	11-57
set radio-profile dtim-interval	11-58
set radio-profile frag-threshold	11-59
set radio-profile max-rx-lifetime	11-61
set radio-profile max-tx-lifetime	11-62
set radio-profile mode	11-63
set radio-profile preamble-length	11-66
set radio-profile qos-mode	11-66
set radio-profile rfid-mode	11-68
set radio-profile rts-threshold	11-69
set radio-profile service-profile	11-70
set radio-profile wmm	11-76

For information about...	Refer to page...
set radio-profile wmm-powersave	11-77
set service-profile attr	11-78
set service-profile auth-dot1x	11-80
set service-profile auth-fallthru	11-82
set service-profile auth-psk	11-84
set service-profile beacon	11-85
set service-profile cac-mode	11-86
set service-profile cac-session	11-87
set service-profile cipher-ccmp	11-88
set service-profile cipher-tkip	11-89
set service-profile cipher-wep104	11-90
set service-profile cipher-wep40	11-91
set service-profile cos	11-92
set service-profile dhcp-restrict	11-93
set service-profile idle-client-probing	11-94
set service-profile keep-initial-vlan	11-95
set service-profile long-retry-count	11-96
set service-profile no-broadcast	11-97
set service-profile proxy-arp	11-99
set service-profile psk-phrase	11-100
set service-profile psk-raw	11-101
set service-profile rsn-ie	11-102
set service-profile shared-key-auth	11-103
set service-profile short-retry-count	11-104
set service-profile soda agent-directory	11-105
set service-profile soda enforce-checks	11-106
set service-profile soda failure-page	11-108
set service-profile soda logout-page	11-109
set service-profile soda mode	11-110
set service-profile soda remediation-acl	11-111
set service-profile soda success-page	11-112
set service-profile ssid-name	11-113
set service-profile ssid-type	11-114
set service-profile static-cos	11-115

For information about...	Refer to page...
set service-profile tkip-mc-time	11-116
set service-profile transmit-rates	11-117
set service-profile user-idle-timeout	11-119
set service-profile web-portal-acl	11-120
set service-profile web-portal-form	11-121
set service-profile web-portal-session-timeout	11-123
set service-profile wep active-multicast-index	11-124
set service-profile wep active-unicast-index	11-125
set service-profile wep key-index	11-126
set service-profile wpa-ie	11-127
show {ap | dap} config	11-128
show {ap | dap} counters	11-132
show {ap | dap} qos-stats	11-135
show {ap | dap} group	11-139
show {ap | dap} status	11-140
show auto-tune attributes	11-145
show auto-tune neighbors	11-147
show dap boot-configuration	11-149
show dap connection	11-151
show dap global	11-153
show dap unconfigured	11-155
show radio-profile	11-157
show service-profile	11-160

clear {ap | dap} radio

Disables an access point radio and resets it to its factory default settings.

Syntax

clear {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2** | **all**}

Parameters

ap *port-list*	List of ports connected to the access point(s) on which to reset a radio.
dap *dap-num*	Number of a Distributed access point on which to reset a radio.
radio 1	Radio 1 of the access point.
radio 2	Radio 2 of the access point. (This option does not apply to single-radio models.)
radio all	All radios on the access point.

Defaults

The **clear ap radio** command resets the radio to the default settings listed in Table 11-1 and in Table 11-4 on page 11-63.

Table 11-1 Radio-Specific Parameters

Parameter	Default Value	Description
antenna-location	indoors	Location of the radio's antenna. This parameter applies only to APs that support external antennas.
antennatype	internal	Enterasys external antenna model. This parameter applies only to AP models that support external antennas.
auto-tune max-power	The highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.	The maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio.
channel	• 802.11b—**6** • 802.11a—Lowest valid channel number for the country of operation	Number of the channel in which a radio transmits and receives traffic
mode	**disable**	Operational state of the radio.
radio-profile	None. You must add the radios to a radio profile.	802.11 settings
tx-power	Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.	Transmit power of a radio, in decibels referred to 1 milliwatt (dBm)

Mode

Enabled

Usage

When you clear a radio, MSS performs the following actions:

- Clears the transmit power, channel, and external antenna setting from the radio.
- Removes the radio from its radio profile and places the radio in the *default* radio profile.

This command does not affect the PoE setting.

Example

The following command disables and resets radio 2 on the access point connected to port 3:

```
RBT-8100# clear ap 3 radio 2
```

Related Commands

- set {ap | dap} radio mode on page 11-38
- set {ap | dap} radio radio-profile on page 11-39

clear dap boot-configuration

Removes the static IP address configuration for a Distributed AP.

Syntax

clear dap boot-configuration *dap-num*

Parameters

dap *dap-num*	Number of the Distributed AP for which you are clearing static IP information.

Defaults

None.

Mode

Enabled.

Usage

When the static IP configuration is cleared for a Distributed AP, the next time the Distributed AP is rebooted, it uses the standard boot process.

Example

The following command clears the static IP address configuration for Distributed AP 1.

```
RBT-8100# clear dap 1 boot-configuration
This will clear specified DAP devices. Would you like to continue? (y/n) [n]y
success: change accepted.
```

Related Commands

- set dap boot-ip on page 11-20
- set dap boot-switch on page 11-22
- set dap boot-vlan on page 11-24
- show dap boot-configuration on page 11-149

clear radio-profile

Removes a radio profile or resets one of the profile's parameters to its default value.

Syntax

clear radio-profile *name* [*parameter*]

Parameters

name	Radio profile name.
parameter	Radio profile parameter: • **beacon-interval** • **dtim-interval** • **countermeasures** • **frag-threshold** • **max-rx-lifetime** • **max-tx-lifetime** • **preamble-length** • **rts-threshold** • **service-profile** (For information about these parameters, see the **set radio-profile** commands that use them.)

Defaults

If you reset an individual parameter, the parameter is returned to the default value listed in Table 11-4 on page 11-63.

Mode

Enabled.

Usage

If you specify a parameter, the setting for the parameter is reset to its default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration. All radios that use this profile must be disabled before you can delete the profile.

Examples

The following commands disable the radios that are using radio profile *rp1* and reset the **beaconed-interval** parameter to its default value:

```
RBT-8100# set radio-profile rp1 mode disable
RBT-8100# clear radio-profile rp1 beacon-interval
success: change accepted.
```

The following commands disable the radios that are using radio profile *rptest* and remove the profile:

```
RBT-8100# set radio-profile rptest mode disable
RBT-8100# clear radio-profile rptest
success: change accepted.
```

Related Commands

- set {ap | dap} radio radio-profile on page 11-39
- set radio-profile mode on page 11-63
- show {ap | dap} config on page 11-128
- show radio-profile on page 11-157

clear service-profile

Removes a service profile or resets one of the profile's parameters to its default value.

Syntax

clear service-profile *name*
[**soda** {**agent-directory** | **failure-page** | **remediation-acl** | **success-page** | **logout-page**}]

Parameters

name	Service profile name.
soda agent-directory	Resets the directory for Sygate On-Demand (SODA) agent files to the default directory. By default, the directory name for SODA agent files is the same as the service profile name.
soda failure-page	Resets the page that is loaded when a client fails the checks performed by the SODA agent. By default, the page is generated dynamically.
soda remediation-acl	Disables use of the specified remediation ACL for the service profile. When no remediation ACL is specified, a client is disconnected form the network when it fails SODA agent checks.
soda success-page	Resets the page that is loaded when a client passes the checks performed by the SODA agent. By default, the page is generated dynamically.
soda logout-page	Resets the page that is loaded when a client logs out of the network. By default, the client is disconnected from the network without a page being loaded.

Defaults

None.

Mode

Enabled.

Usage

If the service profile is mapped to a radio profile, you must remove it from the radio profile first. (After disabling all radios that use the radio profile, use the **clear radio-profile** *name* **service-profile** *name* command.)

Example

The following commands disable the radios that are using radio profile *rp6*, remove service-profile *svcprof6* from *rp6*, then clear *svcprof6* from the configuration.

```
RBT-8100# set radio-profile rp6 mode disable
RBT-8100# clear radio-profile rp6 service-profile svcprof6
success: change accepted.
RBT-8100# clear service-profile svcprof6
success: change accepted.
```

Related Commands

- clear radio-profile on page 11-8
- set radio-profile mode on page 11-63
- show service-profile on page 11-160

reset {ap | dap}

Restarts an access point.

Syntax

reset {**ap** *port-list* | **dap** *dap-num*}

Parameters

ap port-list	List of ports connected to the access points to restart.
dap dap-num	Number of a Distributed access point to reset.

Defaults

None.

Mode

Enabled.

Usage

When you enter this command, the access point drops all sessions and reboots.

Caution: Restarting an access point can cause data loss for users who are currently associated with the access point.

Example

The following command resets the access point on port 7:

```
RBT-8100# reset ap 7
This will reset specified AP devices. Would you like to continue? (y/n)y
success: rebooting ap attached to port 7
```

set dap auto

Creates a profile for automatic configuration of Distributed access points.

Syntax

```
set dap auto
```

Defaults

None.

Mode

Enabled.

Usage

Table 11-2 lists the configurable profile parameters and their defaults. The only parameter that requires configuration is the profile mode. The profile is disabled by default. To use the profile to configure Distributed access points, you must enable the profile using the **set dap auto mode enable** command.

The profile uses the *default* radio profile by default. You can change the profile using the **set dap auto radio radio-profile** command. You can use set dap auto commands to change settings for the parameters listed in Table 11-2. (The commands are listed in the "Related Commands"section.)

Table 11-2 Configurable Profile Parameters for Distributed Access Points

Parameter	Default Value
AP Parameters	
bias	**high**
blink (Not shown in **show dap config** output)	**disable**
force-image-download	**disable** (NO)
group (load balancing group)	none
mode	**disabled**
persistent	none
Radio Parameters	
radio *num* **auto-tune max-power**	**default**
radio *num* **mode**	**enabled**
radio *num* **radio-profile**	**default**
radiotype	**11g** (or **11b** for country codes where 802.11g is not allowed)

Example

The following command creates a profile for automatic Distributed access points configuration:

```
RBT-8100# set dap auto
success: change accepted.
```

Related Commands

- set dap auto mode on page 11-15
- set dap auto persistent on page 11-16
- set dap auto radiotype on page 11-17
- set {ap | dap} bias on page 11-18
- set {ap | dap} blink on page 11-19
- set {ap | dap} group on page 11-28
- set {ap | dap} radio auto-tune max-power on page 11-33
- set {ap | dap} radio auto-tune max-retransmissions on page 11-34
- set {ap | dap} radio auto-tune min-client-rate on page 11-36
- set {ap | dap} radio mode on page 11-38
- set {ap | dap} radio radio-profile on page 11-39
- set {ap | dap} upgrade-firmware on page 11-44

set dap auto mode

Enables a RoamAbout switch's profile for automatic Distributed access point configuration.

Syntax

set dap auto mode {**enable** | **disable**}

Parameters

enable	Enables the access point configuration profile.
disable	Disables the access point configuration profile.

Defaults

The access point configuration profile is disabled by default.

Mode

Enabled.

Usage

You must use the **set dap auto** command to create the profile before you can enable it.

Example

The following command enables the profile for automatic Distributed access point configuration:

```
RBT-8100# set dap auto mode enable
success: change accepted.
```

Related Commands

- set dap auto on page 11-13
- set dap auto persistent on page 11-16
- set dap auto radiotype on page 11-17
- set {ap | dap} bias on page 11-18
- set {ap | dap} blink on page 11-19
- set {ap | dap} group on page 11-28
- set {ap | dap} radio auto-tune max-power on page 11-33
- set {ap | dap} radio auto-tune max-retransmissions on page 11-34
- set {ap | dap} radio auto-tune min-client-rate on page 11-36
- set {ap | dap} radio mode on page 11-38
- set {ap | dap} radio radio-profile on page 11-39
- set {ap | dap} upgrade-firmware on page 11-44

set dap auto persistent

Converts a temporary AP configuration created by the AP configuration profile into a persistent AP configuration on the RoamAbout Switch.

Syntax

set dap auto persistent [*dap-num* | **all**]

Parameters

dap-num	Converts the configuration of the Distributed AP that has the specified connection number into a permanent configuration.
all	Converts the configurations of all Auto-APs being managed by the switch into permanent configurations.

Defaults

None.

Mode

Enabled.

Usage

To display the Distributed AP numbers assigned to Auto-APs, use the **show dap status auto** command.

Example

The following command converts the configuration of Auto-AP 10 into a permanent configuration:

```
RBT-8100# set dap auto persistent 10
success: change accepted.
```

Related Commands

- set dap auto on page 11-13
- set dap auto mode on page 11-15
- set dap auto radiotype on page 11-17

set dap auto radiotype

Sets the radio type for single-access point radios that use the access point configuration profile.

Syntax

```
set dap auto [radiotype {11a | 11b| 11g}]
```

Parameters

radiotype **11a** | **11b** | **11g**	Radio type: • **11a**—802.11a • **11b**—802.11b • **11g**—802.11g

Defaults

The default radio type for model AP3000 is 802.11g.

Usage

If you set the radiotype to **11a** and the AP configuration profile is used to configure a two-radio AP model, radio 1 is configured as an 802.11b/g radio and radio 2 is configured as the 802.11a radio. Because this is the reverse of the standard configuration (where radio 1 is the 802.11a radio and radio 2 is the 802.11b/g radio), the radio 1 settings configured in the AP configuration profile are applied to radio 2. Likewise, the radio 2 settings configured in the profile are applied to radio 1. This behavior ensures that settings for radio 1 are always applied to the 80211a radio, regardless of the radio number.

Example

The following command sets the radio type to 802.11b:

```
RBT-8100# set dap auto radiotype 11b
success: change accepted.
```

Related Commands

- set dap auto on page 11-13
- set dap auto mode on page 11-15
- set dap auto persistent on page 11-16

set {ap | dap} bias

Changes the bias for an access point. Bias is the priority of one RoamAbout switch over other RoamAbout switches for booting and configuring the access point.

Syntax

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}} **bias** {**high** | **low**}

Parameters

ap *port-list*	List of ports on which to change the bias for directly connected access points.
dap *dap-num*	Number of a Distributed access point for which to change the bias.
dap auto	Configures bias for the access point configuration profile. (See set dap auto on page 11-13.)
high	High bias.
low	Low bias.

Defaults

The default bias is high.

Mode

Enabled.

Usage

High bias is preferred over low bias. Bias applies only to RoamAbout switches that are indirectly attached to the access point through an intermediate Layer 2 or Layer 3 network.

If the AP is indirectly connected to RoamAbout switches through the network, the access point boots from the switch with the high bias for the AP. If the bias for all connections is the same, the AP selects the switch that has the greatest capacity to add more active access points.

Access point selection of a RoamAbout switch is *sticky*. After an access point selects a RoamAbout switch to boot from, the AP continues to use that switch for its active data link even if another switch configured with high bias for the access point becomes available.

The following command changes the bias for a Distributed access point to low:

```
RBT-8100# set dap 1 bias low
success: change accepted.
```

Related Commands

show {ap | dap} config on page 11-128

set {ap | dap} blink

Enables or disables LED blink mode on an access point to make it easy to identify. When blink mode is enabled on AP-*xxx* models, the health and radio LEDs alternately blink green and amber.

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}}**blink** {**enable** | **disable**}

Parameters

ap *port-list*	List of ports connected to the access points on which to turn blink mode on or off.
dap *dap-num*	Number of a Distributed access point on which to turn blink mode on or off.
dap auto	Configures blink mode for the access point configuration profile. (See set dap auto on page 11-13.)
enable	Enables blink mode.
disable	Disables blink mode.

Defaults

LED blink mode is disabled by default.

Mode

Enabled.

Usage

Changing the LED blink mode does not alter operation of the access point. Only the behavior of the LEDs is affected.

Example

The following command enables LED blink mode on the access points connected to ports 3 and 4:

```
RBT-8100# set ap 3-4 blink enable
success: change accepted.
```

set dap boot-ip

Specifies static IP address information for a Distributed AP.

Syntax

set dap *dap-num* **boot-ip ip** *ip-addr* **netmask** *mask-addr* **gateway** *gateway-addr* [**mode** {**enable** | **disable**}]

set dap *dap-num* **boot-ip mode** {**enable** | **disable**}

set dap *dap-num* **boot-ip mode** {**enable** | **disable**}

Parameters

dap *dap-num*	Number of the Distributed AP for which you are specifying static IP information.
ip *ip-addr*	The IP address to be assigned to the AP, in dotted decimal notation (for example, 10.10.10.10).
netmask *mask-addr*	The subnet mask, in dotted decimal notation (for example, 255.255.255.0).
gateway *gateway-addr*	The IP address of the next-hop router, in dotted decimal notation.
mode {**enable** | **disable**}	Enables or disables the static IP address for the AP.

Defaults

By default APs use DHCP to obtain an IP address, rather than a using a manually assigned IP address.

Mode

Enabled.

Usage

Normally, Distributed APs use DHCP to obtain IP address information. In some installations, DHCP may not be available. In this case, you can assign static IP address information to the AP, including the AP's IP address and netmask, and default gateway.

If the manually assigned IP information is incorrect, the AP uses DHCP to obtain its IP address.

Example

The following command configures Distributed AP 1 to use IP address 172.16.0.42 with a 24-bit netmask, and use 172.16.0.20 as its default gateway:

```
RBT-8100# set dap 1 boot-ip ip 172.16.0.42 netmask 255.255.255.0 gateway
172.16.0.20 mode en
success: change accepted.
```

Related Commands

- clear dap boot-configuration on page 11-7
- set dap boot-switch on page 11-22
- set dap boot-vlan on page 11-24
- show dap boot-configuration on page 11-149

set dap boot-switch

Specifies the RoamAbout Switch a Distributed AP contacts and attempts to use as its boot device.

Syntax

set dap *dap-num* **boot-switch** [**switch-ip** *ip-addr*] [**name** *name* **dns** *ip-addr*] [**mode** {**enable** | **disable**}]

Parameters

dap *dap-num*	Number of the Distributed AP for which you are specifying static IP information.
switch-ip *ip-addr*	The IP address of the RoamAbout Switch the Distributed AP should boot from.
name *name*	The fully qualified domain name of the RoamAbout Switch the Distributed AP should boot from. When both a name and a switch-ip are specified, the AP uses the name.
dns *ip-addr*	The IP address of the DNS server used to resolve the specified name of the RoamAbout Switch.
mode {**enable** | **disable**}	Enables or disables the AP using the specified boot device.

Defaults

By default APs use the process described in "Default AP Boot Process", in the *RoamAbout Mobility System Software Configuration Guide* to boot from an RoamAbout Switch, instead of using a manually specified RoamAbout Switch.

Mode

Enabled.

Usage

When you specify a boot switch for a distributed AP to boot from, it boots using the process described in "AP Boot Process Using Static IP Configuration", in the *RoamAbout Mobility System Software Configuration Guide.*

When a static IP address is specified for a Distributed AP, there is no preconfigured DNS information or DNS name for the RoamAbout Switch the Distributed AP attempts to use as its boot device. If you configure a static IP address for a Distributed AP, but do not specify a boot device, then the RoamAbout Switch must be reachable via subnet broadcast.

Examples

The following command configures Distributed AP 1 to use the RoamAbout Switch with address 172.16.0.21 as its boot device.

```
RBT-8100# set dap 1 boot-switch switch-ip 172.16.0.21 mode enable
success: change accepted.
```

The following command configures Distributed AP 1 to use the RoamAbout Switch with the name ras2 as its boot device. The DNS server at 172.16.0.1 is used to resolve the name of the RoamAbout Switch.

```
RBT-8100# set dap 1 boot-switch name ras2 dns 172.16.0.1 mode enable
success: change accepted.
```

Related Commands

- clear dap boot-configuration on page 11-7
- set dap boot-ip on page 11-20
- set dap boot-vlan on page 11-24
- show dap boot-configuration on page 11-149

set dap boot-vlan

Specifies 802.1Q VLAN tagging information for a Distributed AP.

Syntax

```
set dap dap-num boot-vlan vlan-tag tag-value [mode {enable | disable}]

set dap dap-num boot-vlan mode {enable | disable}
```

Parameters

dap *dap-num*	Number of the Distributed AP for which you are specifying VLAN information.
vlan-tag *tag-value*	The VLAN tag value. You can specify a number from 1 – 4095.
mode {**enable** | **disable**}	Enables or disables use of the specified VLAN tag on the Distributed AP.

Defaults

None.

Mode

Enabled.

Usage

When this command is configured, all Ethernet frames emitted from the Distributed AP are formatted with an 802.1Q tag with a specified VLAN number. Frames sent to the Distributed AP that are not tagged with this value are ignored.

Example

The following command configures Distributed AP 1 to use VLAN tag 100:

```
RBT-8100# set dap 1 boot-vlan vlan-tag 100 mode enable
success: change accepted.
```

Related Commands

- clear dap boot-configuration on page 11-7
- set dap boot-ip on page 11-20
- set dap boot-switch on page 11-22
- show dap boot-configuration on page 11-149

set {ap | dap} contact

Specifies contact information for an AP.

Syntax

set {**ap** *port-list* | **dap** {*dap-num*} **contact** *string*

Parameters

ap port-list	List of ports on which to specify contact information for directly connected APs.
dap *dap-num*	Number of a Distributed AP for which to specify contact information.
contact *string*	Contact information for the AP. If the contact information includes spaces, enclose the string in quotes.

Defaults

None.

Mode

Enabled.

Usage

Use this command to specify an individual or department to contact for information or maintenance on the AP.

Example

The following command specifies the contact person for AP 7 as *Bob the IT guy*.

```
RBT-8100# set ap 7 contact 'Bob the IT guy'
success: change accepted.
```

Related Commands

show {ap | dap} config on page 11-128

set {ap | dap} image on page 11-29

set dap fingerprint

Verifies an AP's fingerprint on a RoamAbout switch. If AP-RoamAbout Switch security is required by a RoamAbout switch, an AP can establish a management session with the switch only if you have verified the AP's identity by verifying its fingerprint on the switch.

Note: The AP3000 does not require a fingerprint.

Syntax

set dap *num* **fingerprint** *hex*

Parameters

dap *dap-num*	Number of the Distributed AP whose fingerprint you are verifying.
hex	The 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the access point.

Defaults

None.

Mode

Enabled.

Usage

APs are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the access point, in the following format:

```
RSA
aaaa:aaaa:aaaa:aaaa:
aaaa:aaaa:aaaa:aaaa
```

If an AP is already installed and operating, you can use the **show dap status** command to display the fingerprint. The **show dap config** command lists an AP's fingerprint only if the fingerprint has been verified in MSS. If the fingerprint has not been verified, the fingerprint information in the command output is blank.

Example

The following example verifies the fingerprint for Distributed AP 8:

```
RBT-8100# set dap 8 fingerprint b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
success: change accepted.
```

Related Commands

- set dap security on page 11-42
- show {ap | dap} config on page 11-128
- show {ap | dap} status on page 11-140

set {ap | dap} force-image-download

Configures an AP to download its software image from the RoamAbout Switch instead of loading the image that is locally stored on the AP.

Syntax

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}} **force-image-download** {**enable** | **disable**}

ap *port-list*	The list of AP access ports.
dap *dap-num*	The number of a Distributed AP.
dap auto	Configures forced image download for the AP configuration profile. (Refer to "set dap auto" on page 11-13.)
force-image-download enable	Enables forced image download.
force-image-download disable	Disables forced image download.

Defaults

Forced image download is disabled by default.

Mode

Enabled.

Usage

A change to the forced image download option takes place the next time the AP is restarted.

Even when forced image download is disabled (the default), the AP still checks with the RoamAbout Switch to verify that the AP has the latest image, and to verify that the RoamAbout Switch is running MSS Version 5.0 or later.

The AP loads its local image only if the RoamAbout Switch is running MSS Version 5.0 or later and does not have a newer AP image than the one in the AP's local storage. If the switch is not running MSS Version 5.0 or later, or the RoamAbout Switch has a newer version of the AP image than the version in the AP's local storage, the AP loads its image from the RoamAbout Switch.

Example

The following command enables forced image download on Distributed AP 69:

```
RBT-8100# set dap 69 force-image-download enable
success: change accepted.
```

Related Commands

show {ap | dap} config on page 11-128

set {ap | dap} group

Configures a named group of access points. MSS automatically load balances sessions among the access points in a group. To balance the sessions, MSS rejects an association request for an access point's radio if that radio has at least four more active sessions than the radio of the same type with the least number of active sessions within the group.

Syntax

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}} **group** *name*

Parameters

ap *port-list*	List of access point access ports to add to the group.
dap *dap-num*	Number of a Distributed access point to add to the group.
dap auto	Configures an access point group for the access point configuration profile. (Refer to set dap auto on page 11-13.)
name	Access point group name of up to 16 alphanumeric characters, with no spaces.

Defaults

Access points are not grouped by default.

Mode

Enabled.

Usage

You can assign any subset or all of the access points connected to a RoamAbout switch to a group on that switch. All access points in a group must be connected to the same RoamAbout switch.

If you use the name *none*, spelled in any combination of capital or lowercase letters, the specified access point is cleared from all access point groups.

Example

The following command configures an access point group named *loadbalance1* that contains the access points on ports 1, 4, and 7:

```
RBT-8100# set ap 1,4,7 group loadbalance1
success: change accepted.
```

The following command removes the access point on port 4 from all access point groups:

```
RBT-8100# set ap 4 group none
success: change accepted.
```

Related Commands

- show {ap | dap} config on page 11-128
- show {ap | dap} group on page 11-139

set {ap | dap} image

Loads an AirDefense image on an AP.

set {ap | dap} location

Specifies location information for an AP.

Syntax

set {**ap** *port-list* | **dap** {*dap-num*} **location** *string*

Parameters

ap *port-list*	List of ports on which to specify location information for directly connected APs.
dap *dap-num*	Number of a Distributed AP for which to specify location information.
location *string*	Location information for the AP. If the location information includes spaces, enclose the string in quotes.

Defaults

None.

Mode

Enabled.

Usage

Use this command to specify information about the location of the AP.

Example

The following command specifies the location of AP 7 as *The conference room*.

```
RBT-8100# set ap 7 location 'The conference room'
success: change accepted.
```

Related Commands

- show {ap | dap} config on page 11-128
- set {ap | dap} contact on page 11-25

set {ap | dap} name

Changes an access point name.

Syntax

set {**ap** *port-list* | **dap** *dap-num*} **name** *name*

Parameters

ap *port-list*	List of ports connected to the access point to rename.
dap *dap-num*	Number of a Distributed access point to rename.
name	Alphanumeric string of up to 16 characters, with no spaces.

Defaults

The default name of a Distributed access point is based on the number you assign to it when you configure the connection. For example, the default name for Distributed access point 1 is *DAP01*.

Mode

Enabled.

Example

The following command changes the name of the access point on port 1 to *techpubs*:

```
RBT-8100# set ap 1 name techpubs
success: change accepted.
```

Related Commands

show {ap | dap} config on page 11-128

set {ap | dap} radio antenna-location

Specifies the location (indoors or outdoors) of an external antenna. Use this command to ensure that the proper set of channels is available on the radio. In some cases, the set of valid channels for a radio differs depending on whether the antenna is located indoors or outdoors.

Syntax

set {**ap** *port-list* | **dap** *dap-num*} **antenna-location** {**indoors** | **outdoors**}

ap *port-list*	A list of ports connected to the AP access point to rename.
dap *dap-num*	The number of a Distributed AP to rename.
indoors	Specifies that the external antenna is installed indoors (inside the building).
outdoors	Specifies that the external antenna is installed outdoors.

Defaults

The default antenna location is **indoors**.

Mode

Enabled.

Example

The following command sets the antenna location for radio 1 on Distributed AP 22 to **outdoors**:

```
RBT-8100# set dap 22 radio 1 antenna-location outdoors
success: change accepted.
```

Related Commands

set {ap | dap} radio antennatype on page 11-32

set {ap | dap} radio antennatype

Sets the model number for an external antenna.

Syntax

```
set {ap port-list | dap dap-num} radio {1 | 2} antennatype
{ANT1060 | ANT1120 | ANT1180 | ANT5060 | ANT5120 | ANT5180}
```

Parameters

ap *port-list*	List of ports connected to the access points on which to set the channel.
dap *dap-num*	Number of a Distributed AP on which to set the channel.
radio 1	Radio 1 of the AP.
radio 2	Radio 2 of the AP.
antennatype	• Specifies the antenna model number. • internal—Uses the internal antenna instead.

The CLI antenna selections used for the RBT-1602, and their corresponding Enterasys part number are listed in Table 11-3.

Table 11-3 CLI Antenna Selections

CLI Antenna Selection	Enterasys Antenna Part Number
ANT1060	RBTES-BG-S1060
ANT1120	RBTES-BG-S07120
ANT1180	RBTES-BG-S06180
ANT5060	RBTES-AW-S1460
ANT5120	RBTES-AW-S12120
ANT5180	RBTES-AW-S10180

Defaults

All radios use the internal antenna by default, if the AP model has an internal antenna.

Mode

Enabled.

Example

The following command configures the 802.11b/g radio on Distributed AP 1 to use antenna model ANT1060:

```
RBT-8100# set dap 1 radio 1 antennatype ANTxxx
```

set {ap | dap} radio auto-tune max-power

Sets the maximum power that RF Auto-Tuning can set on a radio.

Syntax

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}} **radio** {**1** | **2**} **auto-tune max-power** *power-level*

Parameters

ap *port-list*	List of ports connected to the access points on which to set the maximum power.
dap *dap-num*	Number of a Distributed access point on which to set the maximum power.
dap auto	Sets the maximum power for radios configured by the access point configuration profile. (See set dap auto on page 11-13.)
radio 1	Radio 1 of the access point.
radio 2	Radio 2 of the access point. (This option does not apply to single-radio models.)
power-level	Maximum power setting RF Auto-Tuning can assign to the radio, expressed as the number of decibels in relation to 1 milliwatt (dBm). You can specify a value from 1 up to the maximum value allowed for the country of operation. The *power-level* can be a value from 1 to 20.

Defaults

The default maximum power setting that RF Auto-Tuning can set on a radio is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Mode

Enabled.

Example

The following command sets the maximum power that RF Auto-Tuning can set on radio 1 on the access point on port 7 to 12 dBm.

```
RBT-8100# set ap 7 radio 1 auto-tune max-power 12
success: change accepted.
```

Related Commands

- set radio-profile auto-tune power-config on page 11-52
- set radio-profile auto-tune power-interval on page 11-53

set {ap | dap} radio auto-tune max-retransmissions

Deprecated in MSS Version 5.0.

set {ap | dap} radio auto-tune min-client-rate

Deprecated in MSS Version 5.0. To configure radio transmit rates, refer to “set service-profile transmit-rates” on page 11-117.

set {ap | dap} radio channel

Sets an access point radio's channel.

Syntax

set {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **channel** *channel-number*

Parameters

ap *port-list*	List of ports connected to the access points on which to set the channel.
dap *dap-num*	Number of a Distributed access point on which to set the channel.
radio 1	Radio 1 of the access point.
radio 2	Radio 2 of the access point. (This option does not apply to single-radio models.)
channel *channel-number*	Channel number. The valid channel numbers depend on the country of operation.

Defaults

The default channel depends on the radio type:

- The default channel number for 802.11b/g is 6.
- The default channel number for 802.11a is the lowest valid channel number for the country of operation.

Mode

Enabled.

Usage

You can configure a radio's transmit power on the same command line. Use the **tx-power** option.

This command is not valid if dynamic channel tuning (RF Auto-Tuning) is enabled.

Example

The following command configures the channel on the 802.11a radio on the access point connected to port 5:

```
RBT-8100# set ap 5 radio 1 channel 36
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the access point connected to port 11:

```
RBT-8100# set ap 11 radio 1 channel 1 tx-power 10
success: change accepted.
```

Related Commands

- set {ap | dap} radio tx-power on page 11-40
- show {ap | dap} config on page 11-128

set {ap | dap} radio auto-tune min-client-rate

Sets the minimum rate at which a radio is allowed to transmit traffic to clients. The radio automatically increases its transmit power when necessary to maintain at least the minimum rate with an associated client.

Syntax

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}} **radio** {**1** | **2**} **auto-tune min-client-rate** *rate*

Parameters

ap *port-list*	List of ports connected to the access points on which to set the minimum data rate.
dap *dap-num*	Number of a Distributed access point on which to set the minimum data rate.
dap auto	Sets the radio mode for access points managed by the access point configuration profile. (See set dap auto on page 11-13.)
radio 1	Radio 1 of the access point.
radio 2	Radio 2 of the access point. (This option does not apply to single-radio models.)
rate	Minimum data rate, in megabits per second (Mbps). The valid values depend on the radio type: • For 802.11g radios—**54**, **48**, **36**, **24**, **18**, **12**, **11**, **9**, **6**, **5.5**, **2**, or **1** • For 802.11b radios—**11**, **5.5**, **2**, or **1** • For 802.11a radios—**54**, **48**, **36**, **24**, **18**, **12**, **9**, or **6**

Defaults

The default minimum data transmit rate depends on the radio type:

- The default minimum data rate for 802.11b/g and 802.11b radios is 5.5 Mbps.
- The default minimum data rate for 802.11a radios is 24 Mbps.

Mode

Enabled.

Usage

If the data rate for traffic sent by a radio to an associated client falls below the default minimum rate, the radio increases power, in 1 dBm increments, until all clients are at or above the minimum rate.

After all clients are at or above the minimum data transmit rate, the radio reduces power by 1 dBm. As long as the radio continues to transmit at the minimum data rate or higher for all clients, the radio continues reducing power in 1 dBm increments until it returns to its normal power level.

Note: A radio also can increase power, in 1 dBm increments, if more than the allowed percentage of packets received by the radio from a client are retransmissions. After a radio increases power, all clients must be at the minimum data rate or higher *and* the maximum retransmissions must be within the allowed percentile, before the radio begins reducing power again.

Example

The following command increases the minimum data rate on radio 1, which is an 802.11b/g radio on the access point access port on port 7, to 11 Mbps.

```
RBT-8100# set ap 7 radio 1 min-client-rate 11
success: change accepted.
```

Related Commands

- set radio-profile auto-tune power-backoff-timer on page 11-51
- set radio-profile auto-tune power-config on page 11-52

set {ap | dap} radio mode

Enables or disables a radio on an access point.

Syntax

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}} **radio** {**1** | **2**} **mode** {**enable** | **disable**}

Parameters

ap *port-list*	List of ports connected to the access point(s) on which to turn a radio on or off.
dap *dap-num*	Number of a Distributed access point on which to turn a radio on or off.
dap auto	Sets the radio mode for access points managed by the access point configuration profile. (See set dap auto on page 11-13.)
radio 1	Radio 1 of the access point.
radio 2	Radio 2 of the access point. (This option does not apply to single-radio models.)
mode enable	Enables a radio.
mode disable	Disables a radio.

Defaults

Access point radios are disabled by default.

Mode

Enabled.

Usage

To enable or disable one or more radios to which a profile is assigned, use the **set ap radio radio-profile** command. To enable or disable all radios that use a specific radio profile, use the **set radio-profile** command.

Example

The following command enables radio 1 on the access points connected to ports 1 through 5:

```
RBT-8100# set ap 1-5 radio 1 mode enable
success: change accepted.
```

The following command enables radio 2 on ports 1 through 3:

```
RBT-8100# set ap 1-3 radio 2 mode enable
success: change accepted.
```

Related Commands

- clear {ap | dap} radio on page 11-5
- set {ap | dap} radio radio-profile on page 11-39
- set radio-profile mode on page 11-63
- show {ap | dap} config on page 11-128

set {ap | dap} radio radio-profile

Assigns a radio profile to an access point radio and enables or disables the radio.

Syntax

```
set {ap port-list | dap {dap-num | auto}} radio {1 | 2} radio-
profile name mode {enable | disable}
```

Parameters

ap *port-list*	List of ports.
dap *dap-num*	Number of a Distributed access point.
dap auto	Sets the radio profile for the access point configuration profile. (See set dap auto on page 11-13.)
radio 1	Radio 1 of the access point.
radio 2	Radio 2 of the access point. (This option does not apply to single-radio models.)
radio-profile *name*	Radio profile name of up to 16 alphanumeric characters, with no spaces.
mode enable	Enables radios on the specified ports with the parameter settings in the specified radio profile.
mode disable	Disables radios on the specified ports.

Defaults

None.

Mode

Enabled.

Usage

When you create a new profile, the radio parameters in the profile are set to their factory default values.

To enable or disable all radios that use a specific radio profile, use **set radio-profile**.

Example

The following command enables radio 1 on ports 5 through 8 assigned to radio profile *rp1*:

```
RBT-8100# set ap 5-8 radio 1 radio-profile rp1 mode enable
success: change accepted.
```

Related Commands

- clear {ap | dap} radio on page 11-5
- set {ap | dap} radio mode on page 11-38
- set radio-profile mode on page 11-63
- show radio-profile on page 11-157

set {ap | dap} radio tx-power

Sets an access point radio's transmit power.

Syntax

set {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **tx-power** *power-level*

Parameters

ap *port-list*	List of ports connected to the access points on which to set the transmit power.
dap *dap-num*	Number of a Distributed access point on which to set the transmit power.
radio 1	Radio 1 of the access point.
radio 2	Radio 2 of the access point. (This option does not apply to single-radio models.)
tx-power *power-level*	Number of decibels in relation to 1 milliwatt (dBm). The valid values depend on the country of operation. **Note:** The maximum transmit power you can configure on any Enterasys Networks radio is the maximum allowed for the country in which you plan to operate the radio *or* one of the following values if that value is less than the country maximum: on an 802.11a radio, 11 dBm for channel numbers less than or equal to 64, or 10 dBm for channel numbers greater than 64; on an 802.11b/g radio, 16 dBm for all valid channel numbers for 802.11b, or 14 dBm for all valid channel numbers for 802.11g.

Defaults

The default transmit power on all access point radio types is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Mode

Enabled.

Usage

You also can configure a radio's channel on the same command line. Use the **channel** option.

This command is not valid if dynamic power tuning (RF Auto-Tuning) is enabled.

Example

The following command configures the transmit power on the 802.11a radio on the access point connected to port 5:

```
RBT-8100# set ap 5 radio 1 tx-power 10
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the access point connected to port 11:

```
RBT-8100# set ap 11 radio 1 channel 1 tx-power 10
success: change accepted.
```

Related Commands

- set {ap | dap} radio channel on page 11-35
- show {ap | dap} config on page 11-128

set dap security

Sets security requirements for management sessions between a RoamAbout switch and its Distributed access points.

Note: The maximum transmission unit (MTU) for encrypted access point management traffic is 1498 bytes, whereas the MTU for unencrypted management traffic is 1474 bytes. Make sure the devices in the intermediate network between the RoamAbout switch and Distributed access point can support the higher MTU.

Syntax

```
set dap security {require | optional | none}
```

Parameters

require	Requires all Distributed APs to have encryption keys that have been verified in the CLI by an administrator. If an AP does not have an encryption key or the key has not been verified, the RoamAbout switch does not establish a management session with the AP.
optional	Allows APs to be managed by the switch even if they do not have encryption keys or their keys have not been verified by an administrator. Encryption is used for APs that support it.
none	Encryption is not used, even if the AP supports it.

Defaults

The default setting is **optional**.

Mode

Enabled.

Usage

This parameter applies to all Distributed APs managed by the switch. If you change the setting to **required**, the switch requires Distributed APs to have encryption keys. The switch also requires their fingerprints to be verified in MSS. When AP security is required, an AP can establish a management session with the RoamAbout switch only if its fingerprint has been verified by you in MSS.

A change to access point security support does not affect management sessions that are already established. To apply the new setting to an access point, restart the access point.

Example

The following command configures a RoamAbout to require Distributed access points to have encryption keys:

```
RBT-8100# set dap security require
```

Related Commands

- set dap fingerprint on page 11-26

- show {ap | dap} config on page 11-128
- show {ap | dap} status on page 11-140

set {ap | dap} upgrade-firmware

Disables or reenables automatic upgrade of an access point's boot firmware.

Syntax

set {**ap** *port-list* | **dap** {*dap-num* | **auto**}} **upgrade-firmware** {**enable** | **disable**}

Parameters

ap *port-list*	List of ports connected to the access point(s) on which to allow automatic firmware upgrades.
dap *dap-num*	Number of a Distributed access point on which to allow automatic firmware upgrades.
dap auto	Configures firmware upgrades for the access point configuration profile. (See set dap auto on page 11-13.)
enable	Enables automatic firmware upgrades.
disable	Disables automatic firmware upgrades.

Defaults

Automatic firmware upgrades of access points are enabled by default.

Mode

Enabled.

Usage

When the feature is enabled on a RoamAbout switch port, an access point connected to that port upgrades its boot firmware to the latest version stored on the RoamAbout switch while booting.

Example

The following command disables automatic firmware upgrades on the access point connected to port 9:

```
RBT-8100# set ap 9 upgrade-firmware disable
```

Related Commands

show {ap | dap} config on page 11-128

set radio-profile active-scan

Disables or reenables active RF detection scanning on the access point radios managed by a radio profile. When active scanning is enabled, access point radios look for rogue devices by sending *probe any* requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Passive scanning is always enabled and cannot be disabled. During passive scanning, radios look for rogues by listening for beacons and probe responses.

Syntax

set radio-profile *name* **active-scan** {**enable** | **disable**}

Parameters

name	Radio profile name.
enable	Configures radios to actively scan for rogues.
disable	Configures radios to scan only passively for rogues by listening for beacons and probe responses.

Defaults

Active scanning is enabled by default.

Mode

Enabled.

Usage

You can enter this command on any RoamAbout switch in the Mobility Domain. The command takes effect only on that switch.

Example

The following command disables active scan in radio profile *radprof3*:

```
RBT-8100# set radio-profile radprof3 active-scan disable
success: change accepted.
```

Related Commands

show radio-profile on page 11-157

set radio-profile auto-tune channel-config

Disables or reenables dynamic channel tuning (RF Auto-Tuning) for the access point radios in a radio profile.

Syntax

set radio-profile *name* **auto-tune channel-config** {**enable** | **disable**} [**no-client**]

Parameters

name	Radio profile name.
enable	Configures radios to dynamically select their channels when the radios are started.
disable	Configures radios to use their statically assigned channels, or the default channels if unassigned, when the radios are started.
no-client	Configures radios to change channels regardless of client status. Without this option, a radio changes the channel only if the radio does not have any active clients on that channel.

Defaults

Dynamic channel assignment is enabled by default.

Mode

Enabled.

Usage

If you disable RF Auto-Tuning for channels, MSS does not dynamically set the channels when radios are first enabled and also does not tune the channels during operation.

If RF Auto-Tuning for channels is enabled, MSS does not allow you to manually change channels.

Even when RF Auto-Tuning for channels is enabled, MSS does not change the channel on radios that have active client sessions, unless you use the **no-client** option.

RF Auto-Tuning of channels on 802.11a radios uses only the bottom eight channels in the band (36, 40, 44, 48, 52, 56, 60, and 64). To use a higher channel number, you must disable RF Auto-Tuning of channels on the radio profile the radio is in, and use the **set {ap | dap} radio channel** command to statically configure the channel.

Example

The following command disables dynamic channel tuning for radios in the *rp2* radio profile:

```
RBT-8100# set radio-profile rp2 auto-tune channel-config disable
success: change accepted.
```

Related Commands

- set radio-profile auto-tune channel-holddown on page 11-48
- set radio-profile auto-tune channel-interval on page 11-49

- set radio-profile auto-tune power-config on page 11-52
- show radio-profile on page 11-157

set radio-profile auto-tune channel-holddown

Sets the minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference.

Syntax

set radio-profile *name* **auto-tune channel-holddown** *holddown*

Parameters

name	Radio profile name.
rate	Minimum number of seconds a radio must remain on its current channel setting before RF Auto-Tuning is allowed to change the channel. You can specify from 0 to 65535 seconds.

Defaults

The default RF Auto-Tuning channel holddown is 900 seconds.

Mode

Enabled.

Usage

The channel holddown applies even if RF anomalies occur that normally cause an immediate channel change.

Example

The following command changes the channel holddown for radios in radio profile *rp2* to 600 seconds:

```
RBT-8100# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

Related Commands

- set radio-profile auto-tune channel-config on page 11-46
- set radio-profile auto-tune channel-lockdown on page 11-50
- set radio-profile auto-tune channel-interval on page 11-49
- show radio-profile on page 11-157

set radio-profile auto-tune channel-interval

Sets the interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

Syntax

set radio-profile *name* **auto-tune channel-interval** *seconds*

Parameters

name	Radio profile name.
seconds	Number of seconds RF Auto-Tuning waits before changing radio channels to adjust to RF changes, if needed. You can specify from 0 to 65535 seconds.

Defaults

The default channel interval is 3600 seconds (one hour).

Mode

Enabled.

Usage

Enterasys Networks recommends that you use an interval of at least 300 seconds (5 minutes).

RF Auto-Tuning can change a radio's channel before the channel interval expires in response to RF anomalies. Even in this case, channel changes cannot occur more frequently than the channel holddown interval.

If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.

Example

The following command sets the channel interval for radios in radio profile *rp2* to 2700 seconds (45 minutes):

```
RBT-8100# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

Related Commands

- set radio-profile auto-tune channel-config on page 11-46
- set radio-profile auto-tune channel-holddown on page 11-48
- set radio-profile auto-tune channel-lockdown on page 11-50
- show radio-profile on page 11-157

set radio-profile auto-tune channel-lockdown

Locks down the current channel settings on all radios in a radio profile. The channel settings that are in effect when the command is entered are changed into statically configured channel assignments on the radios. RF Auto-Tuning of channels is then disabled in the radio profile.

Syntax

set radio-profile *name* **auto-tune channel-lockdown**

Parameters

name	Radio profile name.

Defaults

By default, when RF Auto-Tuning of channels is enabled, channels continue to be changed dynamically based on network conditions.

Mode

Enabled.

Usage

To save this command and the static channel configuration commands created when you enter this command, save the configuration.

Example

The following command locks down the channel settings for radios in radio profile *rp2*:

```
RBT-8100# set radio-profile rp2 auto-tune channel-lockdown
success: change accepted.
```

Related Commands

- set radio-profile auto-tune channel-config on page 11-46
- set radio-profile auto-tune channel-holddown on page 11-48
- set radio-profile auto-tune channel-interval on page 11-49
- set radio-profile auto-tune power-lockdown on page 11-54
- show radio-profile on page 11-157

set radio-profile auto-tune power-backoff-timer

Deprecated in MSS Version 5.0.

set radio-profile auto-tune power-config

Enables or disables dynamic power tuning (RF Auto-Tuning) for the access point radios in a radio profile.

Syntax

set radio-profile *name* **auto-tune power-config** {**enable** | **disable**}

Parameters

name	Radio profile name.
enable	Configures radios to dynamically set their power levels when the access points are started.
disable	Configures radios to use their statically assigned power levels, or the default power levels if unassigned, when the radios are started.

Defaults

Dynamic power assignment is disabled by default.

Mode

Enabled.

Usage

When RF Auto-Tuning for power is disabled, MSS does not dynamically set the power levels when radios are first enabled and also does not tune power during operation with associated clients.

When RF Auto-Tuning for power is enabled, MSS does not allow you to manually change the power level.

Example

The following command enables dynamic power tuning for radios in the *rp2* radio profile:

```
RBT-8100# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

Related Commands

- set {ap | dap} radio auto-tune max-power on page 11-33
- set radio-profile auto-tune channel-config on page 11-46
- set radio-profile auto-tune power-interval on page 11-53
- set radio-profile auto-tune channel-lockdown on page 11-50
- set radio-profile auto-tune power-lockdown on page 11-54
- show radio-profile on page 11-157

set radio-profile auto-tune power-interval

Sets the interval at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

Syntax

set radio-profile *name* **auto-tune power-interval** *seconds*

Parameters

name	Radio profile name.
seconds	Number of seconds MSS waits before changing radio power levels to adjust to RF changes, if needed. You can specify from 1 to 65535 seconds.

Defaults

The default power tuning interval is 300 seconds.

Mode

Enabled.

Example

The following command sets the power interval for radios in radio profile *rp2* to 240 seconds:

```
RBT-8100# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

Related Commands

- set {ap | dap} radio auto-tune max-power on page 11-33
- set radio-profile auto-tune power-config on page 11-52
- set radio-profile auto-tune power-lockdown on page 11-54
- set radio-profile auto-tune power-ramp-interval on page 11-55
- show radio-profile on page 11-157

set radio-profile auto-tune power-lockdown

Locks down the current power settings on all radios in a radio profile. The power settings that are in effect when the command is entered are changed into statically configured power settings on the radios. RF Auto-Tuning of power is then disabled in the radio profile.

Syntax

set radio-profile *name* **auto-tune power-lockdown**

Parameters

name	Radio profile name.

Defaults

By default, when RF Auto-Tuning of power is enabled, power settings continue to be changed dynamically based on network conditions.

Mode

Enabled.

Usage

To save this command and the static power configuration commands created when you enter this command, save the configuration.

Example

The following command locks down the power settings for radios in radio profile *rp2*:

```
RBT-8100# set radio-profile rp2 auto-tune power-lockdown
success: change accepted.
```

Related Commands

- set {ap | dap} radio auto-tune max-power on page 11-33
- set radio-profile auto-tune channel-lockdown on page 11-50
- set radio-profile auto-tune power-config on page 11-52
- set radio-profile auto-tune power-interval on page 11-53
- set radio-profile auto-tune power-ramp-interval on page 11-55
- show radio-profile on page 11-157

set radio-profile auto-tune power-ramp-interval

Changes the interval at which power is increased or decreased, in 1 dBm increments, on radios in a radio profile until the optimum power level calculated by RF Auto-Tuning is reached.

Syntax

set radio-profile *name* **auto-tune power-ramp-interval** *seconds*

Parameters

name	Radio profile name.
seconds	Number of seconds MSS waits before increasing or decreasing radio power by another 1 dBm. You can specify from 1 to 65535.

Defaults

The default interval is 60 seconds.

Mode

Enabled.

Example

The following command changes the power ramp interval for radios in radio profile *rp2* to 120 seconds:

```
RBT-8100# set radio-profile rp2 auto-tune power-ramp-interval 120
success: change accepted.
```

Related Commands

- set {ap | dap} radio auto-tune max-power on page 11-33
- set radio-profile auto-tune power-config on page 11-52
- set radio-profile auto-tune power-interval on page 11-53
- set radio-profile auto-tune power-lockdown on page 11-54
- show radio-profile on page 11-157

set radio-profile beacon-interval

Changes the rate at which each access point radio in a radio profile advertises its service set identifier (SSID).

Syntax

set radio-profile *name* **beacon-interval** *interval*

Parameters

name	Radio profile name.
interval	Number of milliseconds (ms) between beacons. You can specify from 25 ms to 8191 ms.

Defaults

The beacon interval for access point radios is 100 ms by default.

Mode

Enabled.

Usage

You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Example

The following command changes the beacon interval for radio profile *rp1* to 200 ms:

```
RBT-8100# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- show radio-profile on page 11-157

set radio-profile countermeasures

Caution: Countermeasures affect wireless service on a radio. When an access point radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.

Enables or disables countermeasures on the access point radios managed by a radio profile. Countermeasures are packets sent by a radio to prevent clients from being able to use rogue access points.

Access point radios can also issue countermeasures against interfering devices. An interfering device is not part of the Enterasys network but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any RoamAbout switch in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with access point radios.

Syntax

set radio-profile *name* **countermeasures** {**all** | **rogue**}

Parameters

name	Radio profile name.
all	Configures radios to attack rogues and interfering devices.
rogue	Configures radios to attack rogues only.

Defaults

Countermeasures are disabled by default.

Mode

Enabled.

Examples

The following command enables countermeasures in radio profile *radprof3* for rogues only:

```
RBT-8100# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The following command disables countermeasures in radio profile *radprof3*:

```
RBT-8100# clear radio-profile radprof3 countermeasures
success: change accepted.
```

set radio-profile dtim-interval

Changes the number of times after every beacon that each access point radio in a radio profile sends a delivery traffic indication map (DTIM). An access point sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM.

Note: The DTIM interval applies to both the beaconed SSID and the nonbeaconed SSID.

Syntax

set radio-profile *name* **dtim-interval** *interval*

Parameters

name	Radio profile name.
interval	Number of times the DTIM is transmitted after every beacon. You can enter a value from 1 through 31.

Defaults

By default, access points send the DTIM once after each beacon.

Mode

Enabled.

Usage

You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The DTIM interval does not apply to unicast frames.

Example

The following command changes the DTIM interval for radio profile *rp1* to 2:

```
RBT-8100# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- show radio-profile on page 11-157
- show radio-profile on page 11-157

set radio-profile frag-threshold

Changes the fragmentation threshold for the AP radios in a radio profile. The fragmentation threshold is the threshold at which the long-retry-count is applicable instead of the short-retry-count.

The long-retry-count specifies the number of times a radio can send a unicast frame that is equal to or longer than the frag-threshold without receiving an acknowledgment.

The short-retry-count specifies the number of times a radio can send a unicast frame that is shorter than the frag-threshold without receiving an acknowledgment.

Syntax

set radio-profile *name* **frag-threshold** *threshold*

Parameters

name	Radio profile name.
threshold	Maximum frame length, in bytes. You can enter a value from 256 through 2346.

Defaults

The default fragmentation threshold for access point radios is 2346 bytes.

Mode

Enabled.

Usage

You must disable all radios that are using a radio profile before you can change parameters in the profile. Use set radio-profile mode on page 11-63.

The frag-threshold does not specify the maximum length a frame is allowed to be without being broken into multiple frames before transmission. Enterasys APs do not support fragmentation upon transmission, only upon reception.

The frag-threshold does not change the RTS threshold, which specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. To change the RTS threshold, use set radio-profile rts-threshold on page 11-69 instead.

Example

The following command changes the fragmentation threshold for radio profile *rp1* to 1500 bytes:

```
RBT-8100# set radio-profile rp1 frag-threshold 1500
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- set radio-profile rts-threshold on page 11-69
- set service-profile long-retry-count on page 11-96
- set service-profile short-retry-count on page 11-104
- show radio-profile on page 11-157

set radio-profile max-rx-lifetime

Changes the maximum receive threshold for the access point radios in a radio profile. The maximum receive threshold specifies the number of milliseconds that a frame *received* by a radio can remain in buffer memory.

Syntax

set radio-profile *name* **max-rx-lifetime** *time*

Parameters

name	Radio profile name.
time	Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults

The default maximum receive threshold for access point radios is 2000 ms (2 seconds).

Mode

Enabled.

Usage

You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Example

The following command changes the maximum receive threshold for radio profile *rp1* to 4000 ms:

```
RBT-8100# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- set radio-profile max-tx-lifetime on page 11-62
- show radio-profile on page 11-157

set radio-profile max-tx-lifetime

Changes the maximum transmit threshold for the access point radios in a radio profile. The maximum transmit threshold specifies the number of milliseconds that a frame *scheduled to be transmitted* by a radio can remain in buffer memory.

Syntax

set radio-profile *name* **max-tx-lifetime** *time*

Parameters

name	Radio profile name.
time	Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults

The default maximum transmit threshold for access point radios is 2000 ms (2 seconds).

Mode

Enabled.

Usage

You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Example

The following command changes the maximum transmit threshold for radio profile *rp1* to 4000 ms:

```
RBT-8100# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- set radio-profile max-rx-lifetime on page 11-61
- show radio-profile on page 11-157

set radio-profile mode

Creates a new radio profile, or disables or reenables all access point radios that are using a specific profile.

Syntax

```
set radio-profile name [mode {enable | disable}]
```

Parameters

radio-profile *name*	Radio profile name of up to 16 alphanumeric characters, with no spaces. Use this command without the **mode enable** or **mode disable** option to create a new profile.
mode enable	Enables the radios that use this profile.
mode disable	Disables the radios that use this profile.

Defaults

Each radio profile that you create has a set of properties with factory default values that you can change with the other **set radio-profile** commands in this chapter. Table 11-4 lists the parameters controlled by a radio profile and their default values.

Table 11-4 Defaults for Radio Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
active-scan	**enable**	Sends *probe any* requests (probe requests with a null SSID name) to solicit probe responses from other access points.
auto-tune	**enable**	Allows dynamic configuration of channel and power settings by MSS.
beacon-interval	**100**	Waits 100 ms between beacons.
countermeasures	Not configured	Does not issue countermeasures against any device.
dtim-interval	**1**	Sends the delivery traffic indication map (DTIM) after every beacon.
frag-threshold	**2346**	Uses the short-retry-count for frames shorter than 2346 bytes and uses the long-retry-count for frames that are 2346 bytes or longer.
max-rx-lifetime	**2000**	Allows a received frame to stay in the buffer for up to 2000 ms (2 seconds).
max-tx-lifetime	**2000**	Allows a frame that is scheduled for transmission to stay in the buffer for up to 2000 ms (2 seconds).
preamble-length	**short**	Advertises support for short 802.11b preambles, accepts either short or long 802.11b preambles, and generates unicast frames with the preamble length specified by the client. **Note:** This parameter applies only to 802.11b/g radios.

Table 11-4 Defaults for Radio Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
qos-mode	**wmm**	Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of AP radios for Wi-Fi Multimedia (WMM).
rfid-mode	**disable**	Radio does not function as a location receiver in an AeroScout Visibility System.
rts-threshold	**2346**	Transmits frames longer than 2346 bytes by means of the Request-to-Send/Clear-to-Send (RTS/CTS) method.
service-profile	No service profiles defined	You must configure a service profile. The service profile sets the SSID name and other parameters.
wmm-powersave	**disable**	Requires clients to send a separate PSpoll to retrieve each unicast packet buffered by the AP radio.

Mode

Enabled.

Usage

Use the command without any optional parameters to create new profile. If the radio profile does not already exist, MSS creates a new radio profile. Use the **enable** or **disable** option to enable or disable all the radios using a profile. To assign the profile to one or more radios, use the **set ap radio radio-profile** command.

To change a parameter in a radio profile, you must first disable all the radios in the profile. After you complete the change, you can reenable the radios.

To enable or disable specific radios without disabling all of them, use the **set ap radio** command.

Examples

The following command configures a new radio profile named *rp1*:

```
RBT-8100# set radio-profile rp1
success: change accepted.
```

The following command enables the radios that use radio profile *rp1*:

```
RBT-8100# set radio-profile rp1 mode enable
```

The following commands disable the radios that use radio profile *rp1*, change the beacon interval, then reenable the radios:

```
RBT-8100# set radio-profile rp1 mode disable
RBT-8100# set radio-profile rp1 beacon-interval 200
RBT-8100# set radio-profile rp1 mode enable
```

The following command enables the WPA IE on access point radios in radio profile *rp2*:

```
RBT-8100# set radio-profile rp2 wpa-ie enable
success: change accepted.
```

Related Commands

- set {ap | dap} radio mode on page 11-38
- set {ap | dap} radio radio-profile on page 11-39
- show {ap | dap} config on page 11-128
- show radio-profile on page 11-157

set radio-profile preamble-length

Changes the preamble length for which an 802.11b/g access point radio advertises support. This command does not apply to 802.11a.

Syntax

set radio-profile *name* **preamble-length** {**long** | **short**}

Parameters

name	Radio profile name.
long	Advertises support for long preambles.
short	Advertises support for short preambles.

Defaults

The default is short.

Mode

Enabled.

Usage

Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (**short** or **long**), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

If a client associated with an 802.11b/g radio uses long preambles for unicast traffic, the access point still accepts frames with short preambles but does not transmit frames with short preambles. This change also occurs if the access point overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Example

The following command configures 802.11b/g radios that use the radio profile *rp_long to* advertise support for long preambles instead of short preambles:

```
RBT-8100# set radio-profile rp_long preamble-length long
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- show radio-profile on page 11-157

set radio-profile qos-mode

Sets the prioritization mode for forwarding queues on AP radios managed by the radio profile.

Syntax

set radio-profile *name* **qos-mode** {**svp** | **wmm**}

Parameters

svp	Optimizes forwarding prioritization of AP radios for SpectraLink Voice Priority (SVP).
wmm	Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of AP radios for Wi-Fi Multimedia (WMM).

Defaults

The default QoS mode is **wmm**.

Mode

Enabled.

Usage

When SVP is enabled, AP forwarding prioritization is optimized for SpectraLink Voice Priority (SVP) instead of WMM, and the AP does not tag packets it sends to the RoamAbout Switch. Otherwise, classification and tagging remain in effect. (For information, see the "Configuring Quality of Service" chapter of the *RoamAbout Mobility System Software Configuration Guide*.)

If you plan to use SVP or another non-WMM type of prioritization, you must configure ACLs to tag the packets. (See the "Enabling Prioritization for Legacy Voice over IP" section in the "Configuring and Managing Security ACLs" chapter of the *RoamAbout Mobility System Software Configuration Guide*.)

Example

The following command changes the QoS mode for radio profile *rp1* to SVP:

```
RBT-8100# set radio-profile rp1 qos-mode svp
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- show radio-profile on page 11-157

set radio-profile rfid-mode

Enables AP radios managed by a radio profile to function as location receivers in an AeroScout Visibility System. An AeroScout Visibility System allows system administrators to track mobile assets using RFID tags.

When you enable RFID mode on a radio profile, radios in the profile can receive and process signals transmitted by RFID tags and relay them with related information to the AeroScout Engine. If the floor plan is modeled in RoamAbout Switch Manager, you also can use RoamAbout Switch Manager to display the locations of assets.

Syntax

set radio-profile *name* **rfid-mode** {**enable** | **disable**}

Parameters

name	Radio profile name.
enable	Enables radios to function as asset location receivers.
disable	Disables radios from functioning as asset location receivers.

Defaults

The default is **disable**.

Mode

Enabled.

Example

The following command enables radios managed by radio profile *rp1* to act as asset location receivers:

```
RBT-8100# set radio-profile rfid-mode enable
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- show radio-profile on page 11-157

set radio-profile rts-threshold

Changes the RTS threshold for the access point radios in a radio profile. The RTS threshold specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.

Syntax

set radio-profile *name* **rts-threshold** *threshold*

Parameters

name	Radio profile name.
threshold	Maximum frame length, in bytes. You can enter a value from 256 through 3000.

Defaults

The default RTS threshold for an access point radio is 2346 bytes.

Mode

Enabled.

Usage

You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Example

The following command changes the RTS threshold for radio profile *rp1* to 1500 bytes:

```
RBT-8100# set radio-profile rp1 rts-threshold 1500
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- show radio-profile on page 11-157

set radio-profile service-profile

Maps a service profile to a radio profile. All radios that use the radio profile also use the parameter settings, including SSID and encryption settings, in the service profile.

Syntax

set radio-profile *name* **service-profile** *name*

Parameters

radio-profile *name*	Radio profile name of up to 16 alphanumeric characters, with no spaces.
service-profile *name*	Service profile name of up to 16 alphanumeric characters, with no spaces.

Defaults

A radio profile does not have a service profile associated with it by default. In this case, the radios in the radio profile use the default settings for parameters controlled by the service profile. Table 11-5 lists the parameters controlled by a service profile and their default values.

Table 11-5 Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
attr	No attributes configured	Does not assign the SSID's authorization attribute values to SSID users, even if attributes are not otherwise assigned.
auth-dot1x	**enable**	When the Wi-Fi Protected Access (WPA) information element (IE) is enabled, uses 802.1X to authenticate WPA clients.
auth-fallthru	**none**	Denies access to users who do not match an 802.1X or MAC authentication rule for the SSID requested by the user.
auth-psk	**disable**	Does not support using a preshared key (PSK) to authenticate WPA clients.
beacon	**enable**	Sends beacons to advertise the SSID managed by the service profile.
cac-mode	**none**	Does not limit the number of active user sessions based on Call Admission Control (CAC).
cac-session	**14**	If session-based CAC is enabled (**cac-mode** is set to **session**), limits the number of active user sessions on a radio to 14.
cipher-ccmp	**disable**	Does not use Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to encrypt traffic sent to WPA clients.

Table 11-5 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
cipher-tkip	**enable**	When the WPA IE is enabled, uses Temporal Key Integrity Protocol (TKIP) to encrypt traffic sent to WPA clients.
cipher-wep104	**disable**	Does not use Wired Equivalent Privacy (WEP) with 104-bit keys to encrypt traffic sent to WPA clients.
cipher-wep40	**disable**	Does not use WEP with 40-bit keys to encrypt traffic sent to WPA clients.
cos	**0**	If static CoS is enabled (**static-cos** is set to **enable**), assigns CoS 0 to all data traffic to or from clients.
dhcp-restrict	**disable**	Does not restrict a client's traffic to only DHCP traffic while the client is being authenticated and authorized.
idle-client-probing	**enable**	Sends a keepalive packet (a null-data frame) to each client every 10 seconds.
keep-initial-vlan	**disable**	Reassigns the user to a VLAN after roaming, instead of leaving the roamed user on the VLAN assigned by the switch where the user logged on. Enabling this option does not retain the user's initial VLAN assignment in all cases. (For information, see "set service-profile keep-initial-vlan" on page 11-95.)
long-retry-count	**5**	Sends a long unicast frame up to five times without acknowledgment.
no-broadcast	**disable**	Does not reduce wireless broadcast traffic by sending unicasts to clients for ARP requests and DHCP Offers and Acks instead of forwarding them as multicasts.
proxy-arp	**disable**	Does not reply on behalf of wireless clients to ARP requests for client IP addresses. Instead, the radio forwards the ARP Requests as wireless broadcasts.
psk-phrase	No passphrase defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.

Table 11-5 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
psk-raw	No preshared key defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
rsn-ie	**disable**	Does not use the RSN IE in transmitted frames. (The RSN IE is required for 802.11i. RSN is sometimes called *WPA2*.)
shared-key-auth	**disable**	Does not use shared-key authentication. This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the **set radio-profile auth-psk** command.
short-retry-count	**5**	Sends a short unicast frame up to five times without acknowledgment.
soda	**disable**	Sygate On Demand Agent (SODA) files are not downloaded to connecting clients.
ssid-name	**enterasys**	Uses the SSID name *enterasys*.
static-cos	**disable**	Assigns CoS based on the QoS mode (**wmm** or **svp**) or based on ACLs.
ssid-type	**crypto**	Encrypts wireless traffic for the SSID.
tkip-mc-time	**60000**	Uses Michael countermeasures for 60,000 ms (60 seconds) following detection of a second MIC failure within 60 seconds.
transmit-rates	802.11a: • mandatory: **6.0**,**12.0**,**24.0** • beacon-rate: **6.0** • multicast-rate: **auto** • disabled: none 802.11b: • mandatory: **1.0**,**2.0** • beacon-rate: **2.0** • multicast-rate: **auto** • disabled: none 802.11g: • mandatory: **1.0**,**2.0**,**5.5**,**11.0** • beacon-rate: **2.0** • multicast-rate: **auto** • disabled: none	Accepts associations only from clients that support one of the mandatory rates. Sends beacons at the specified rate (6 Mbps for 802.11a, 2 Mbps for 802.11b/g). Sends multicast data at the highest rate that can reach all clients connected to the radio. Accepts frames from clients at all valid data rates. (No rates are disabled by default.)

Table 11-5 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
user-idle-timeout	**180**	Allows a client to remain idle for 180 seconds (3 minutes) before MSS changes the client's session to the Disassociated state.
web-portal-acl	**portalacl** This is the default only if the fallthru type on the service profile has been set to **web-portal**. Otherwise, the value is unconfigured.	If set to **portalacl** and the service profile fallthru is set to **web-portal**, radios use the *portalacl* ACL to filter traffic for Web Portal users during authentication. If the fallthru type is **web-portal** but **web-portal-acl** is set to an ACL other than *portalacl*, the other ACL is used. If the fallthru type is not **web-portal**, radios do not use the **web-portal-acl** setting.
web-portal-form	Not configured	For WebAAA users, serves the Enterasys Networks login page.
web-portal-session-timeout	**5**	Allows a Web Portal WebAAA session to remain in the Deassociated state 5 seconds before being terminated automatically.
wep key-index	No keys defined	Uses dynamic WEP rather than static WEP. **Note:** If you configure a WEP key for static WEP, MSS continues to also support dynamic WEP.
wep active-multicast-index	**1**	Uses WEP key 1 for static WEP encryption of multicast traffic if WEP encryption is enabled and keys are defined.
wep active-unicast-index	**1**	Uses WEP key 1 for static WEP encryption of unicast traffic if WEP encryption is enabled and keys are defined.
wpa-ie	**disable**	Does not use the WPA IE in transmitted frames.

Mode

Enabled.

Usage

You must configure the service profile before you can map it to a radio profile. You can map the same service profile to more than one radio profile.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Example

The following command maps service-profile *wpa_clients* to radio profile *rp2*:

```
RBT-8100# set radio-profile rp2 service-profile wpa_clients
success: change accepted.
```

Related Commands

- set service-profile attr on page 11-78
- set service-profile auth-dot1x on page 11-80
- set service-profile auth-fallthru on page 11-82
- set service-profile auth-psk on page 11-84
- set service-profile beacon on page 11-85
- set service-profile cac-mode on page 11-86
- set service-profile cac-session on page 11-87
- set service-profile cipher-ccmp on page 11-88
- set service-profile cipher-tkip on page 11-89
- set service-profile cipher-wep104 on page 11-90
- set service-profile cipher-wep40 on page 11-91
- set service-profile cos on page 11-92
- set service-profile dhcp-restrict on page 11-93
- set service-profile idle-client-probing on page 11-94
- set service-profile long-retry-count on page 11-96
- set service-profile no-broadcast on page 11-97
- set service-profile proxy-arp on page 11-99
- set service-profile psk-phrase on page 11-100
- set service-profile psk-raw on page 11-101
- set service-profile rsn-ie on page 11-102
- set service-profile shared-key-auth on page 11-103
- set service-profile short-retry-count on page 11-104
- set service-profile soda mode on page 11-110
- set service-profile ssid-name on page 11-113
- set service-profile ssid-type on page 11-114
- set service-profile static-cos on page 11-115
- set service-profile tkip-mc-time on page 11-116
- set service-profile transmit-rates on page 11-117
- set service-profile user-idle-timeout on page 11-119
- set service-profile web-portal-form on page 11-121

- set service-profile web-portal-session-timeout on page 11-123
- set service-profile wep active-multicast-index on page 11-124
- set service-profile wep active-unicast-index on page 11-125
- set service-profile wep key-index on page 11-126

set radio-profile wmm

Deprecated in MSS Version 4.2. To enable or disable WMM, refer to “set radio-profile qos-mode” on page 11-67.

set radio-profile wmm-powersave

Enables Unscheduled Automatic Powersave Delivery (U-APSD) on AP radios managed by the radio profile. U-APSD enables WMM clients that use powersave mode to more efficiently request buffered unicast packets from AP radios.

When U-APSD is enabled, a client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority. U-APSD can be enabled for individual traffic priorities, for individual clients, based on the client's request. A client enables U-APSD for a traffic priority by indicating this preference when (re)associating with the AP radio.

A client can but is not required to request U-APSD for all four traffic priorities. The AP radio still buffers packets for all traffic priorities even if the client does not request U-APSD for them. However, to retrieve buffered packets for priorities that are not using U-APSD, a client must send a separate PSpoll for each buffered packet.

Syntax

set radio-profile *name* **wmm-powersave** {**enable** | **disable**}

Parameters

name	Radio profile name.
enable	Enables U-APSD.
disable	Disables U-APSD.

Defaults

U-APSD is disabled by default.

Mode

Enabled.

Usage

U-APSD is supported only for QoS mode WMM. If WMM is not enabled on the radio profile, use the **set radio-profile qos-mode** command to enable it.

Example

The following command enables U-APSD on radio profile *rp1*:

```
RBT-8100# set radio-profile rp1 wmm-powersave enable
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- set radio-profile qos-mode on page 11-67
- show radio-profile on page 11-157

set service-profile attr

Configures authorization attributes that are applied by default to users accessing the SSID managed by the service profile. These SSID default attributes are applied in addition to any supplied by the RADIUS server or from the local database.

Syntax

set service-profile *name* **attr** *attribute-name value*

Parameters

name	Service profile name.
attribute-name value	Name and value of an attribute you are using to authorize SSID users for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 8-1 on page 8-45. All of the attributes listed in Table 8-1 can be used with this command except **ssid**.

Defaults

By default, a service profile does not have any authorization attributes set.

Mode

Enabled.

Usage

To change the value of a default attribute for a service profile, use the set **service-profile attr** command and specify a new value. To delete an attribute, use the **<???>** command.

The SSID default attributes are applied *in addition* to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy rules also take precedence over SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

For example, a service profile might be configured with the **service-type** attribute set to *2*. If a user accessing the SSID is authenticated by a RADIUS server, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then that user will have a total of two attributes set: **service-type** and **vlan-name**.

If the service profile is configured with the **vlan-name** attribute set to *blue*, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then the attribute from the RADIUS server takes precedence; the user is placed in the orange VLAN.

You can display the attributes for each connected user and whether they are set through AAA or through SSID defaults by entering the **show sessions network verbose** command. You can display the configured SSID defaults by entering the **show service-profile** command.

Examples

The following command assigns users accessing the SSID managed by service profile *sp2* to VLAN *blue.*

```
RBT-8100# set service-prof sp2 attr vlan-name blue
success: change accepted.
```

The following command assigns users accessing the SSID managed by service profile *sp2* to the Mobility Profile *tulip.*

```
RBT-8100# set service-prof sp2 attr mobility-profile tulip
success: change accepted.
```

The following command limits the days and times when users accessing the SSID managed by service profile *sp2* can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
RBT-8100# set service-prof sp2 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.
```

Related Commands

- show service-profile on page 11-160
- show sessions network on page 18-7

set service-profile auth-dot1x

Disables or reenables 802.1X authentication of Wi-Fi Protected Access (WPA) clients by access point radios, when the WPA information element (IE) is enabled in the service profile that is mapped to the radio profile that the radios are using.

Syntax

set service-profile *name* a**uth-dot1x** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables 802.1X authentication of WPA clients.
disable	Disables 802.1X authentication of WPA clients.

Defaults

When the WPA IE is enabled, 802.1X authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-dot1x** setting has no effect.

Mode

Enabled.

Usage

This command does not disable dynamic WEP for non-WPA clients. To disable dynamic WEP for non-WPA clients, enable the WPA IE (if not already enabled) and disable the 40-bit WEP and 104-bit WEP cipher suites in the WPA IE, if they are not already disabled.

To use 802.1X authentication for WPA clients, you also must enable the WPA IE.

If you disable 802.1X authentication of WPA clients, the only method available for authenticating the clients is preshared key (PSK) authentication. To use this, you must enable PSK support and configure a passphrase or key.

Example

The following command disables 802.1X authentication for WPA clients that use service profile *wpa_clients*:

```
RBT-8100# set service-profile wpa_clients auth-dot1x disable
success: change accepted.
```

Related Commands

- set service-profile auth-psk on page 11-84
- set service-profile psk-phrase on page 11-100
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile auth-fallthru

Specifies the authentication type for users who do not match an 802.1X or MAC authentication rule for an SSID managed by the service profile. When a user tries to associate with an SSID, MSS checks the authentication rules for that SSID for a userglob that matches the username. If the SSID does not have an authentication rule that matches the username, authentication for the user *falls through* to the fallthru type.

The fallthru type is a service profile parameter, and applies to all radios within the radio profiles that are mapped to the service profile.

Syntax

set service-profile *name* **auth-fallthru** {**last-resort** | **none** | **web-portal**}

Parameters

last-resort	Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password.
none	Denies authentication and prohibits the user from accessing the SSID. **Note:** The fallthru authentication type **none** is different from the authentication method **none** you can specify for administrative access. The fallthru authentication type **none** denies access to a network user. In contrast, the authentication method **none** allows access to the RoamAbout switch by an administrator. (Refer to "set authentication admin" on page 8-27 and "set authentication console" on page 8-29.)
web-portal	Serves the user a web page from the RoamAbout switch's nonvolatile storage for secure login to the network.

Defaults

The default fallthru authentication type is **none**.

If a username does not match a userglob in an authentication rule for the SSID requested by the user, the RoamAbout switch that is managing the radio the user is connected to redirects the user to a web page located on the RoamAbout switch. The user must type a valid username and password on the web page to access the SSID.

Mode

Enabled.

Usage

The **last-resort** fallthru authentication type allows any user to access any SSID managed by the service profile. This method does not require the user to provide a username or password. Use the **last-resort** method only if none of the SSIDs managed by the service profile require secure access.

The **web-portal** authentication type also requires additional configuration items. (See the "Configuring AAA for Network Users" chapter of the *RoamAbout Mobility System Software Configuration Guide*.)

Example

The following command sets the fallthru authentication for SSIDS managed by the service profile *rnd_lab* to web-portal:

```
RBT-8100# set service-profile rnd_lab auth-fallthru web-portal
success: change accepted.
```

Related Commands

- set web-portal on page 8-61
- set service-profile web-portal-form on page 11-121
- show service-profile on page 11-160

set service-profile auth-psk

Enables preshared key (PSK) authentication of Wi-Fi Protected Access (WPA) clients by access point radios in a radio profile, when the WPA information element (IE) is enabled in the service profile.

Syntax

set service-profile *name* **auth-psk** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables PSK authentication of WPA clients.
disable	Disables PSK authentication of WPA clients.

Defaults

When the WPA IE is enabled, PSK authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-psk** setting has no effect.

Mode

Enabled.

Usage

This command affects authentication of WPA clients only.

To use PSK authentication, you also must configure a passphrase or key. In addition, you must enable the WPA IE.

Example

The following command enables PSK authentication for service profile *wpa_clients*:

```
RBT-8100# set service-profile wpa_clients auth-psk enable
success: change accepted.
```

Related Commands

- set service-profile auth-dot1x on page 11-80
- set service-profile psk-raw on page 11-101
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile beacon

Disables or reenables beaconing of the SSID managed by the service profile.

An access point radio responds to an 802.11 *probe any* request with only the beaconed SSID(s). For a nonbeaconed SSID, radios respond only to directed 802.11 probe requests that match the nonbeaconed SSID's SSID string.

When you disable beaconing for an SSID, the radio still sends beacon frames, but the SSID name in the frames is blank.

Syntax

set service-profile *name* **beacon** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables beaconing of the SSID managed by the service profile.
disable	Disables beaconing of the SSID managed by the service profile.

Defaults

Beaconing is enabled by default.

Mode

Enabled.

Example

The following command disables beaconing of the SSID managed by service profile *sp2*:

```
RBT-8100# set service-profile sp2 beacon disable
success: change accepted.
```

Related Commands

- set radio-profile beacon-interval on page 11-56
- set service-profile ssid-name on page 11-113
- set service-profile ssid-type on page 11-114
- show service-profile on page 11-160

set service-profile cac-mode

Configures the Call Admission Control (CAC) mode.

Usage

set service-profile *name* **cac-mode** {**none** | **session**}

Parameters

name	Service profile name.
none	CAC is not used.
session	CAC is based on the number of active sessions.

Defaults

The default CAC mode is **none**.

Mode

Enabled.

Example

The following command enables session-based CAC on service profile *sp1*:

```
RBT-8100# set service-profile sp1 cac-mode session
success: change accepted.
```

Related Commands

- set service-profile cac-session on page 11-87
- show service-profile on page 11-160

set service-profile cac-session

Specifies the maximum number of active sessions a radio can have when session-based CAC is enabled. When an AP radio has reached the maximum allowed number of active sessions, the radio refuses connections from additional clients.

Syntax

set service-profile *name* **cac-session** *max-sessions*

Parameters

name	Service profile name.
max-sessions	Maximum number of active sessions allowed on the radio.

Defaults

The default number of sessions allowed is 14.

Mode

Enabled.

Usage

This command applies only when the CAC mode is **session**. If the CAC mode is **none**, you can still change the maximum number of sessions, but the setting does not take effect until you change the CAC mode to **session**. To change the CAC mode, use the **set service-profile cac-mode** command.

Examples

The following command changes the maximum number of sessions for radios used by service profile *sp1* to 10:

```
RBT-8100# set service-profile sp1 cac-session 10
success: change accepted.
```

Related Commands

- set service-profile cac-mode on page 11-86
- show service-profile on page 11-160

set service-profile cipher-ccmp

Enables Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption with WPA clients, for a service profile.

Syntax

set service-profile *name* **cipher-ccmp** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables CCMP encryption for WPA clients.
disable	Disables CCMP encryption for WPA clients.

Defaults

CCMP encryption is disabled by default.

Mode

Enabled.

Usage

To use CCMP, you must also enable the WPA IE.

Example

The following command configures service profile *sp2* to use CCMP encryption:

```
RBT-8100# set service-profile sp2 cipher-ccmp enable
success: change accepted.
```

Related Commands

- set service-profile cipher-tkip on page 11-89
- set service-profile cipher-wep104 on page 11-90
- set service-profile cipher-wep40 on page 11-91
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile cipher-tkip

Disables or reenables Temporal Key Integrity Protocol (TKIP) encryption in a service profile.

Syntax

set service-profile *name* **cipher-tkip** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables TKIP encryption for WPA clients.
disable	Disables TKIP encryption for WPA clients.

Defaults

When the WPA IE is enabled, TKIP encryption is enabled by default.

Mode

Enabled.

Usage

To use TKIP, you must also enable the WPA IE.

Example

The following command disables TKIP encryption in service profile *sp2*:

```
RBT-8100# set service-profile sp2 cipher-tkip disable
success: change accepted.
```

Related Commands

- set service-profile cipher-ccmp on page 11-88
- set service-profile cipher-wep104 on page 11-90
- set service-profile cipher-wep40 on page 11-91
- set service-profile tkip-mc-time on page 11-116
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile cipher-wep104

Enables dynamic Wired Equivalent Privacy (WEP) with 104-bit keys, in a service profile.

Syntax

set service-profile *name* **cipher-wep104** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables 104-bit WEP encryption for WPA clients.
disable	Disables 104-bit WEP encryption for WPA clients.

Defaults

104-bit WEP encryption is disabled by default.

Mode

Enabled.

Usage

To use 104-bit WEP with WPA clients, you must also enable the WPA IE.

When 104-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 40-bit dynamic WEP, you must enable WEP with 40-bit keys. Use the **set service-profile cipher-wep40** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Example

The following command configures service profile *sp2* to use 104-bit WEP encryption:

```
RBT-8100# set service-profile sp2 cipher-wep104 enable
success: change accepted.
```

Related Commands

- set service-profile cipher-ccmp on page 11-88
- set service-profile cipher-tkip on page 11-89
- set service-profile cipher-wep40 on page 11-91
- set service-profile wep key-index on page 11-126
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile cipher-wep40

Enables dynamic Wired Equivalent Privacy (WEP) with 40-bit keys, in a service profile.

Syntax

set service-profile *name* **cipher-wep40** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables 40-bit WEP encryption for WPA clients.
disable	Disables 40-bit WEP encryption for WPA clients.

Defaults

40-bit WEP encryption is disabled by default.

Mode

Enabled.

Usage

To use 40-bit WEP with WPA clients, you must also enable the WPA IE.

When 40-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 104-bit dynamic WEP, you must enable WEP with 104-bit keys in the service profile. Use the **set service-profile cipher-wep104** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Example

The following command configures service profile *sp2* to use 40-bit WEP encryption:

```
RBT-8100# set service-profile sp2 cipher-wep40 enable
success: change accepted.
```

Related Commands

- set service-profile cipher-ccmp on page 11-88
- set service-profile cipher-tkip on page 11-89
- set service-profile cipher-wep104 on page 11-90
- set service-profile wep key-index on page 11-126
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile cos

Sets the Class-of-Service (CoS) level for static CoS.

Syntax

set service-profile *name* **cos** *level*

Parameters

name	Service profile name.
level	CoS value assigned by the AP to all traffic in the service profile.

Defaults

The default static CoS level is 0.

Mode

Enabled.

Usage

This command applies only when static CoS is enabled. If static CoS is disabled, prioritization is based on the QoS mode configured in the radio profile, and on any ACLs that set CoS. (See the "Configuring Quality of Service" chapter of the *RoamAbout Mobility System Software Configuration Guide*.) To enable static CoS, use the **set service-profile static-cos** command.

Example

The following command changes the static CoS level to 7 (voice priority):

```
RBT-8100# set service-profile sp1 cos 7
success: change accepted.
```

Related Commands

- set service-profile static-cos on page 11-115
- show service-profile on page 11-160

set service-profile dhcp-restrict

Enables or disables DHCP Restrict on a service profile. DHCP Restrict filters a newly associated client's traffic to allow DHCP traffic only, until the client has been authenticated and authorized. All other traffic is captured by the RoamAbout Switch and is not forwarded. After the client is successfully authorized, the traffic restriction is removed.

Syntax

set service-profile *name* **dhcp-restrict** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables DHCP Restrict.
disable	Disables DHCP Restrict.

Defaults

DHCP Restrict is disabled by default.

Mode

Enabled.

Usage

To further reduce the overhead of DHCP traffic, use the **set service-profile no-broadcast** command to disable DHCP broadcast traffic from AP radios to clients on the service profile's SSID.

Example

The following command enables DHCP Restrict on service profile *sp1*:

```
RBT-8100# set service-profile sp1 dhcp-restrict enable
success: change accepted.
```

Related Commands

- set service-profile no-broadcast on page 11-97
- set service-profile proxy-arp on page 11-99
- show service-profile on page 11-160

set service-profile idle-client-probing

Disables or reenables periodic keepalives from AP radios to clients on a service profile's SSID. When idle-client probing is enabled, the AP radio sends a unicast null-data frame to each client every 10 seconds. Normally, a client that is still active sends an Ack in reply to the keepalive.

If a client does not send any data or respond to any keepalives before the user idle timeout expires, MSS changes the client's session to the Disassociated state.

Syntax

set service-profile *name* **idle-client-probing** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables keepalives.
disable	Disables keepalives.

Defaults

Idle-client probing is enabled by default.

Mode

Enabled.

Usage

The length of time a client can remain idle (unresponsive to idle-client probes) is specified by the **user-idle-timeout** command.

Example

The following command disables idle-client keepalives on service profile *sp1*:

```
RBT-8100# set service-profile sp1 idle-client-probing disable
success: change accepted.
```

Related Commands

- set service-profile user-idle-timeout on page 11-119
- show service-profile on page 11-160

set service-profile keep-initial-vlan

Configures AP radios managed by the radio profile to leave a roamed user on the VLAN assigned by the switch where the user logged on. When this option is disabled, a user's VLAN is reassigned by each RoamAbout Switch to which a user roams.

Syntax

set service-profile *name* **keep-initial-vlan** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables radios to leave a roamed user on the same VLAN instead of reassigning the VLAN.
disable	Configures radios to reassign a roamed user's VLAN.

Defaults

This option is disabled by default.

Mode

Enabled.

Usage

Even when this option is enabled, the RoamAbout Switch to which a user roams (the *roamed-to* switch) can reassign the VLAN in any of the following cases:

- A location policy on the local switch reassigns the VLAN.
- The user is configured in the switch's local database and the VLAN-Name attribute is set on the user or on a user group the user is in.
- The access rule on the roamed-to switch uses RADIUS, and the VLAN-Name attribute is set on the RADIUS server.

Example

The following command enables the **keep-initial-vlan** option on service profile *sp3*:

```
RBT-8100# set service-profile sp3 keep-initial-vlan enable
success: change accepted.
```

Related Commands

show service-profile on page 11-160

set service-profile long-retry-count

Changes the long retry threshold for a service profile. The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is equal to or longer than the frag-threshold.

Syntax

set service-profile *name* **long-retry-count** *threshold*

Parameters

name	Service profile name.
threshold	Number of times the radio can send the same long unicast frame. You can enter a value from 1 through 15.

Defaults

The default long unicast retry threshold is 5 attempts.

Mode

Enabled.

Example

The following command changes the long retry threshold for service profile *sp1* to 8:

```
RBT-8100# set service-profile sp1 long-retry-count 8
success: change accepted.
```

Related Commands

- set radio-profile frag-threshold on page 11-59
- set service-profile short-retry-count on page 11-104
- show service-profile on page 11-160

set service-profile no-broadcast

Disables or reenables the no-broadcast mode. The no-broadcast mode helps reduce traffic overhead on an SSID by leaving more of an SSID's bandwidth available for unicast traffic. The no-broadcast mode also helps VoIP handsets conserve power by reducing the amount of broadcast traffic sent to the phones.

When enabled, the no-broadcast mode prevents AP radios from sending DHCP or ARP broadcasts to clients on the service profile's SSID. Instead, an AP radio handles this traffic as follows:

- ARP requests—If the SSID has clients whose IP addresses the RoamAbout Switch does not already know, the switch allows the AP radio to send the ARP request as a unicast to only those stations whose addresses the switch does not know. The AP radio does not forward the ARP request as a broadcast and does not send the request as a unicast to stations whose addresses the switch already knows.
- DHCP Offers or Acks—If the destination MAC address belongs to a client on the SSID, the AP radio sends the DHCP Offer or Ack as a unicast to that client only.

The no-broadcast mode does not affect other types of broadcast traffic and does not prevent clients from sending broadcasts.

Syntax

set service-profile *name* **no-broadcast** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables the no-broadcast mode. AP radios are not allowed to send broadcast traffic to clients on the service profile's SSID.
disable	Disables the no-broadcast mode.

Defaults

The no-broadcast mode is disabled by default. (Broadcast traffic not disabled.)

Mode

Enabled.

Usage

To further reduce ARP traffic on a service profile, use the **set service-profile proxy-arp** command to enable Proxy ARP.

Example

The following command enables the no-broadcast mode on service profile *sp1*:

```
RBT-8100# set service-profile sp1 no-broadcast enable
success: change accepted.
```

Related Commands

- set service-profile dhcp-restrict on page 11-93
- set service-profile proxy-arp on page 11-99
- show service-profile on page 11-160

set service-profile proxy-arp

Enables proxy ARP. When proxy ARP is enabled, the RoamAbout Switch replies to ARP requests for client IP address on behalf of the clients. This feature reduces broadcast overhead on a service profile's SSID by eliminating ARP broadcasts from AP radios to the SSID's clients.

If the ARP request is for a client whose IP address the switch does not already know, the RoamAbout Switch allows AP radios to send the ARP request to clients. If the no-broadcast mode is also enabled, the AP radios send the ARP request as a unicast to only the clients whose addresses the switch does not know. However, if no-broadcast mode is disabled, the AP radios send the ARP request as a broadcast to all clients on the SSID.

Syntax

set service-profile *name* **proxy-arp** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables proxy ARP.
disable	Disables proxy ARP.

Defaults

Proxy ARP is disabled by default.

Mode

Enabled.

Usage

To further reduce broadcast traffic on a service profile, use the **set service-profile no-broadcast** command to disable DHCP and ARP request broadcasts.

Example

The following command enables proxy ARP on service profile *sp1*:

```
RBT-8100# set service-profile sp1 proxy-arp enable
success: change accepted.
```

Related Commands

- set service-profile dhcp-restrict on page 11-93
- set service-profile no-broadcast on page 11-97
- show service-profile on page 11-160

set service-profile psk-phrase

Configures a passphrase for preshared key (PSK) authentication to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax

set service-profile *name* **psk-phrase** *passphrase*

Parameters

name	Service profile name.
passphrase	An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

Defaults

None.

Mode

Enabled.

Usage

MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the RoamAbout switch's configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

Example

The following command configures service profile *sp3* to use passphrase "1234567890123<>?=+&% The quick brown fox jumps over the lazy sl":

```
RBT-8100# set service-profile sp3 psk-phrase "1234567890123<>?=+&% The quick
brown fox jumps over the lazy sl"
success: change accepted.
```

Related Commands

- clear mac-user attr on page 8-12
- set service-profile auth-psk on page 11-84
- set service-profile psk-raw on page 11-101
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile psk-raw

Configures a raw hexadecimal preshared key (PSK) to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax

set service-profile *name* **psk-raw** *hex*

Parameters

name	Service profile name.
hex	A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults

None.

Mode

Enabled.

Usage

MSS converts the hexadecimal number into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the RoamAbout switch's configuration. The binary number is never displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

Example

The following command configures service profile *sp3* to use a raw PSK with PSK clients:

```
RBT-8100# set service-profile sp3 psk-raw
c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
success: change accepted.
```

Related Commands

- set mac-user attr on page 8-44
- set service-profile auth-psk on page 11-84
- set service-profile psk-phrase on page 11-100
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile rsn-ie

Enables the Robust Security Network (RSN) Information Element (IE).

The RSN IE advertises the RSN (sometimes called WPA2) authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax

set service-profile *name* **rsn-ie** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables the RSN IE.
disable	Disables the RSN IE.

Defaults

RSN IE is disabled by default.

Mode

Enabled.

Usage

When the RSN IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

Examples

The following command enables the RSN IE in service profile *sprsn*:

```
RBT-8100# set service-profile sprsn rsn-ie enable
success: change accepted.
```

Related Commands

- set service-profile auth-dot1x on page 11-80
- set service-profile auth-psk on page 11-84
- set service-profile cipher-ccmp on page 11-88
- set service-profile cipher-wep104 on page 11-90
- set service-profile cipher-wep40 on page 11-91
- show service-profile on page 11-160

set service-profile shared-key-auth

Enables shared-key authentication, in a service profile.

Note: Use this command only if advised to do so by Enterasys Networks. This command does not enable preshared key (PSK) authentication for Wi-Fi Protected Access (WPA). To enable PSK encryption for WPA, use set service-profile auth-psk on page 11-84.

Syntax

set service-profile *name* **shared-key-auth** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables shared-key authentication.
disable	Disables shared-key authentication.

Defaults

Shared-key authentication is disabled by default.

Mode

Enabled.

Example

The following command enables shared-key authentication in service profile *sp4*:

```
RBT-8100# set service-profile sp4 shared-key-auth enable
success: change accepted.
```

Related Commands

- set radio-profile mode on page 11-63
- show radio-profile on page 11-157
- show service-profile on page 11-160

set service-profile short-retry-count

Changes the short retry threshold for a service profile. The short retry threshold specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment. A short unicast frame is a frame that is shorter than the frag-threshold.

Syntax

set service-profile *name* **short-retry-count** *threshold*

Parameters

name	Service profile name.
threshold	Number of times a radio can send the same short unicast frame. You can enter a value from 1 through 15.

Defaults

The default short unicast retry threshold is 5 attempts.

Mode

Enabled.

Example

The following command changes the short retry threshold for service profile *sp1* to 3:

```
RBT-8100# set service-profile sp1 short-retry-count 3
success: change accepted.
```

Related Commands

- set radio-profile frag-threshold on page 11-59
- set service-profile long-retry-count on page 11-96
- show service-profile on page 11-160

set service-profile soda agent-directory

Specifies the directory on the RoamAbout Switch where the SODA agent files for a service profile are located.

Syntax

set service-profile *name* **soda agent-directory** *directory*

Parameters

name	Service profile name.
directory	Directory on the RoamAbout Switch for SODA agent files.

Defaults

By default, the RoamAbout Switch expects SODA agent files to be located in a directory with the same name as the service profile.

Mode

Enabled.

Usage

If the same SODA agent is used for multiple service profiles, you can use this command to specify a single directory for SODA agent files on the RoamAbout Switch, rather than placing the same SODA agent files in a separate directory for each service profile.

Example

The following command specifies *soda-agent* as the location for SODA agent files for service profile sp1:

```
RBT-8100# set service-profile sp1 soda agent-directory soda-agent
success: change accepted.
```

Related Commands

- install soda agent on page 20-10
- uninstall soda agent on page 20-30
- show service-profile on page 11-160

set service-profile soda enforce-checks

Specifies whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks.

Syntax

set service-profile *name* **enforce-checks** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	SODA agent checks are performed before the client is allowed access to the network.
disable	Allows the client access to the network immediately after the SODA agent is downloaded, without waiting for the checks to be run.

Defaults

By default, SODA agent checks are performed before the client is allowed access to the network.

Mode

Enabled

Usage

When the SODA agent is enabled in a service profile, by default the SODA agent checks are downloaded to a client and run before the client is allowed on the network. You can use this command to disable the enforcement of the SODA security checks, so that the client is allowed access to the network immediately after the SODA agent is downloaded, rather than waiting for the security checks to be run.

When the enforce checks option is enabled, upon successful completion of the SODA agent checks, the client performs an HTTP Get operation to load the success page. Upon loading the success page, the client is granted access to the network.

In order for the client to load the success page, you must make sure the SODA agent is configured (through SODA Manager) with the correct URL of the success page, so that the RoamAbout Switch can serve the page to the client.

Similarly, you must make sure the SODA agent is configured with the correct URLs of the failure and logout pages, so that when the client requests these pages, the RoamAbout SwitchRoamAbout Switch can serve those pages as well.

Example

The following command allows network access to clients after they have downloaded the SODA agent, but without requiring that the SODA agent checks be completed:

```
RBT-8100# set service-profile sp1 enforce-checks disable
success: change accepted.
```

Related Commands

- set service-profile soda mode on page 11-110
- show service-profile on page 11-160

set service-profile soda failure-page

Specifies a page on the RoamAbout Switch that is loaded when a client fails the security checks performed by the SODA agent.

Syntax

set service-profile *name* **soda failure-page** *page*

Parameters

name	Service profile name.
page	Page that is loaded if the client fails the security checks performed by the SODA agent.

Defaults

By default, the RoamAbout Switch dynamically generates a page indicating that the SODA agent checks have failed.

Mode

Enabled.

Usage

Use this command to specify a custom page that is loaded by the client when the SODA agent checks fail. After this page is loaded, the specified remediation ACL takes effect, or if there is no remediation ACL configured, then the client is disconnected from the network.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

The page is assumed to reside in the root directory on the RoamAbout Switch. You can optionally specify a different directory where the page resides.

Examples

The following command specifies *failure.html* as the page to load when a client fails the SODA agent checks:

```
RBT-8100# set service-profile sp1 soda failure-page failure.html
success: change accepted.
```

The following command specifies *failure.html*, in the *soda-files* directory, as the page to load when a client fails the SODA agent checks:

```
RBT-8100# set service-profile sp1 soda failure-page soda-files/failure.html
success: change accepted.
```

Related Commands

- set service-profile soda enforce-checks on page 11-106
- set service-profile soda remediation-acl on page 11-111
- show service-profile on page 11-160

set service-profile soda logout-page

Specifies a page on the RoamAbout Switch that is loaded when a client logs out of the network by closing the SODA virtual desktop.

Syntax

set service-profile *name* **soda logout-page** *page*

Parameters

name	Service profile name.
page	Page that is loaded when the client closes the SODA virtual desktop.

Defaults

None.

Mode

Enabled.

Usage

When a client closes the SODA virtual desktop, the client is automatically disconnected from the network. You can use this command to specify a page that is loaded when the client closes the SODA virtual desktop.

The client can request this page at any time, to ensure that the client's session has been terminated. You can add the IP address of the RoamAbout Switch to the DNS server as a well-known name, and you can advertise the URL of the page to users as a logout page.

The page is assumed to reside in the root directory on the RoamAbout Switch. You can optionally specify a different directory where the page resides.

Note: You must also enable the HTTPS server on the RoamAbout Switch, so that clients can log out of the network and access the logout page using HTTPS. To do this, use the **set ip https server enable** command.

Examples

The following command specifies *logout.html* as the page to load when a client closes the SODA virtual desktop:

```
RBT-8100# set service-profile sp1 soda logout-page logout.html
success: change accepted.
```

The following command specifies *logout.html*, in the *soda-files* directory, as the page to load when a client closes the SODA virtual desktop:

```
RBT-8100# set service-profile sp1 soda logout-page soda-files/logout.html
success: change accepted.
```

Related Commands

- show service-profile on page 11-160

set service-profile soda mode

Enables or disables Sygate On-Demand (SODA) functionality for a service profile.

Syntax

set service-profile *name* **soda mode** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables SODA functionality for the service profile.
disable	Disables SODA functionality for the service profile.

Mode

Enabled.

Usage

When SODA functionality is enabled for a service profile, a SODA agent is downloaded to clients attempting to connect to an AP managed by the service profile. The SODA agent performs a series of security-related checks on the client; if the client passes the checks, it can be admitted to the network.

In release 4.2, SODA functionality requires that Web Portal WebAAA also be enabled for the service profile.

Example

The following command enables SODA functionality for service profile *sp1*:

```
RBT-8100# set service-profile sp1 soda mode enable
success: change accepted.
```

Related Commands

- install soda agent on page 20-10
- set service-profile soda enforce-checks on page 11-106
- show service-profile on page 11-160

set service-profile soda remediation-acl

Specifies an ACL to be applied to a client if it fails the checks performed by the SODA agent.

Syntax

set service-profile *name* **soda remediation-acl** *acl-name*

Parameters

name	Service profile name.
acl-name	Name of an existing security ACL to use as a remediation ACL for this service profile. ACL names must start with a letter and are case-insensitive.

Defaults

None.

Mode

Enabled.

Usage

If the SODA agent checks fail on a client, by default the client is disconnected from the network. Optionally, you can specify a *failure page* for the client to load (with the **set service-profile soda failure-page** command). When the failure page is loaded, you can optionally specify a *remediation ACL* to apply to the client. The remediation ACL can be used to grant the client limited access to network resources, for example. If there is no remediation ACL configured, then the client is disconnected from the network when the failure page is loaded.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

Example

The following command configures the RoamAbout Switch to apply *acl-1* to a client when it loads the failure page:

```
RBT-8100# set service-profile sp1 soda remediation-acl acl-1
success: change accepted.
```

Related Commands

- set service-profile soda enforce-checks on page 11-106
- set service-profile soda failure-page on page 11-108
- show service-profile on page 11-160

set service-profile soda success-page

Specifies a page on the RoamAbout Switch that is loaded when a client passes the security checks performed by the SODA agent

Syntax

set service-profile *name* **soda success-page** *page*

Parameters

name	Service profile name.
page	Page that is loaded if the client passes the security checks performed by the SODA agent.

Defaults

By default, the RoamAbout Switch generates a page indicating that the client passed the SODA agent checks.

Mode

Enabled.

Usage

Use this command to specify a custom page that is loaded by the client when it passes the checks performed by the SODA agent. After this page is loaded, the client is placed in its assigned VLAN and granted access to the network.

The page is assumed to reside in the root directory on the RoamAbout Switch. You can optionally specify a different directory where the page resides.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

Examples

The following command specifies *success.html*, which resides in the root directory on the RoamAbout Switch, as the page to load when a client passes the SODA agent checks:

```
RBT-8100# set service-profile sp1 soda success-page success.html
success: change accepted.
```

The following command specifies *success.html*, which resides in the *soda-files* directory on the RoamAbout Switch, as the page to load when a client passes the SODA agent checks:

```
RBT-8100# set service-profile sp1 soda success-page soda-files/success.html
success: change accepted.
```

Related Commands

- set service-profile soda enforce-checks on page 11-106
- set service-profile soda mode on page 11-110
- show service-profile on page 11-160

set service-profile ssid-name

Configures the SSID name in a service profile.

Syntax

set service-profile *name* **ssid-name** *ssid-name*

Parameters

name	Service profile name.
ssid-name	Name of up to 32 alphanumeric characters. You can include blank spaces in the name, if you delimit the name with single or double quotation marks. You must use the same type of quotation mark (either single or double) on both ends of the string.

Defaults

The default SSID type is crypto (encrypted) and the default name is *enterasys*.

Mode

Enabled.

Example

The following command applies the name *corporate users* to the SSID managed by service profile *mycorp_srvcprf*:

```
RBT-8100# set service-profile mycorp_srvcprf ssid-name "corporate users"
success: change accepted.
```

Related Commands

- set service-profile ssid-type on page 11-114
- show service-profile on page 11-160

set service-profile ssid-type

Specifies whether the SSID managed by a service profile is encrypted or unencrypted.

Syntax

set service-profile *name* **ssid-type** [**clear** | **crypto**]

Parameters

name	Service profile name.
clear	Wireless traffic for the service profile's SSID is not encrypted.
crypto	Wireless traffic for the service profile's SSID is encrypted.

Defaults

The default SSID type is crypto.

Mode

Enabled.

Example

The following command changes the SSID type for service profile *clear_wlan* to **clear**:

```
RBT-8100# set service-profile clear_wlan ssid-type clear
success: change accepted.
```

Related Commands

- set service-profile ssid-name on page 11-113
- show service-profile on page 11-160

set service-profile static-cos

Enables or disables static CoS on a service profile. Static CoS assigns the same CoS level to all traffic on the service profile's SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any ACLs that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic.

When static CoS is enabled, the standard MSS prioritization mechanism is not used. Instead, the AP sets CoS as follows:

- For traffic from the AP to clients, the AP places the traffic into the forwarding queue that corresponds to the CoS level configured on the service profile. For example, if the static CoS level is set to 7, the AP radio places client traffic in its Voice queue.
- For traffic from clients to the network, the AP marks the DSCP value in the IP headers of the tunnel packets used to carry the user data from the AP to the RoamAbout Switch.

Syntax

set service-profile *name* **static-cos** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables static CoS on the service profile.
disable	Disables static CoS on the service profile.

Defaults

Static CoS is disabled by default.

Mode

Enabled.

Usage

The CoS level is specified by the s**et service-profile cos** command.

Example

The following command enables static CoS on service profile *sp1*:

```
RBT-8100# set service-profile sp1 static-cos enable
success: change accepted.
```

Related Commands

- set service-profile cos on page 11-92
- show service-profile on page 11-160

set service-profile tkip-mc-time

Changes the length of time that access point radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, access point radios dissociate all TKIP and WPA WEP clients and refuse all association and reassociation requests until the countermeasures end.

Syntax

set service-profile *name* **tkip-mc-time** *wait-time*

Parameters

name	Service profile name.
wait-time	Number of milliseconds (ms) countermeasures remain in effect. You can specify from 0 to 60,000.

Defaults

The default countermeasures wait time is 60,000 ms (60 seconds).

Mode

Enabled.

Usage

Countermeasures apply only to TKIP and WEP clients. This includes WPA WEP clients and non-WPA WEP clients. CCMP clients are not affected.

The TKIP cipher suite must be enabled. The WPA IE also must be enabled.

Example

The following command changes the countermeasures wait time for service profile *sp3* to 30,000 ms (30 seconds):

```
RBT-8100# set service-profile sp3 tkip-mc-time 30000
success: change accepted.
```

Related Commands

- set service-profile cipher-tkip on page 11-89
- set service-profile wpa-ie on page 11-127
- show service-profile on page 11-160

set service-profile transmit-rates

Changes the data rates supported by AP radios for a service-profile's SSID.

Syntax

```
set service-profile name transmit-rates {11a | 11b | 11g}
mandatory rate-list [disabled rate-list] [beacon-rate rate] [multicast-rate
{rate | auto}]
```

Parameters

name	Service profile name.
11a | **11b** | **11g**	Radio type.
mandatory *rate-list*	Set of data transmission rates that clients are required to support in order to associate with an SSID on an AP radio. A client must support at least one of the mandatory rates. These rates are advertised in the basic rate set of 802.11 beacons, probe responses, and reassociation response frames sent by AP radios. Data frames and management frames sent by AP radios use one of the specified mandatory rates. The valid rates depend on the radio type: • **11a**—6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0 • **11b**—1.0, 2.0, 5.5, 11.0 • **11g**—1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0 Use a comma to separate multiple rates; for example: **6.0,9.0,12.0**
disabled *rate-list*	Data transmission rates that AP radios will not use to transmit data. This setting applies only to data sent by the AP radios. The radios will still accept frames from clients at disabled data rates. The valid rates depend on the radio type and are the same as the valid rates for **mandatory**.
beacon-rate *rate*	Data rate of beacon frames sent by AP radios. This rate is also used for probe-response frames. The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. However, you cannot set the beacon rate to a disabled rate.
multicast-rate {*rate* | **auto**}	Data rate of multicast frames sent by AP radios. • *rate*—Sets the multicast rate to a specific rate. The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. However, you cannot set the multicast rate to a disabled rate. • **auto**—Sets the multicast rate to the highest rate that can reach all clients connected to the AP radio.

Defaults

This command has the following defaults:

- **mandatory**:
  - 11a—**6.0,12.0,24.0**
  - 11b—**1.0,2.0**
  - 11g—**1.0,2.0,5.5,11.0**
- **disabled**—None. All rates applicable to the radio type are supported by default.
- **beacon-rate**:
  - 11a—**6.0**
  - 11b—**2.0**
  - 11g—**2.0**
- **multicast-rate**—**auto** for all radio types.

Mode

Enabled.

Usage

If you disable a rate, you cannot use the rate as a mandatory rate or the beacon or multicast rate. All rates that are applicable to the radio type and that are not disabled are supported by the radio.

Example

The following command sets 802.11a mandatory rates for service profile *sp1* to 6 Mbps and 9 Mbps, disables rates 48 Mbps and 54 Mbps, and changes the beacon rate to 9 Mbps:

```
RBT-8100# set service-profile sp1 transmit-rates 11a mandatory 6.0,9.0 disabled
48.0,54.0 beacon-rate 9.0
success: change accepted.
```

Related Commands

show service-profile on page 11-160

set service-profile user-idle-timeout

Changes the number of seconds MSS will leave a session up for a client that is not sending data and is not responding to keepalives (idle-client probes). If the timer expires, the client's session is changed to the Dissociated state.

The timer is reset to 0 each time a client sends data or responds to an idle-client probe. If the idle-client probe is disabled, the timer is reset each time the client sends data.

Syntax

set service-profile *name* **user-idle-timeout** *seconds*

Parameters

name	Service profile name.
seconds	Number of seconds a client is allowed to remain idle before MSS changes the session to the Dissociated state. You can specify from 20 to 86400 seconds. To disable the timer, specify 0.

Defaults

The default user idle timeout is 180 seconds (3 minutes).

Mode

Enabled.

Example

The following command increases the user idle timeout to 360 seconds (6 minutes):

```
RBT-8100# set service-profile sp1 user-idle-timeout 360
success: change accepted.
```

Related Commands

- set service-profile idle-client-probing on page 11-94
- set service-profile web-portal-session-timeout on page 11-123
- show service-profile on page 11-160

set service-profile web-portal-acl

Changes the ACL name MSS uses to filter a Web-Portal user's traffic during authentication.

Use this command if you create a custom Web-Portal ACL to allow more than just DHCP traffic during authentication. For example, if you configure an ACL that allows a Web-Portal user to access a credit card server, use this command to use the custom ACL for Web-Portal users that associate with the service profile's SSID.

Syntax

set service-profile *name* **web-portal-acl** *aclname*

Parameters

name	Service profile name.
aclname	Name of the ACL to use for filtering Web-Portal user traffic during authentication.

Defaults

By default, a service profile's **web-portal-acl** option is unset. However, when you change the service profile's **auth-fallthru** option to **web-portal**, MSS sets the **web-portal-acl** option to *portalacl*. (MSS automatically creates the *portalacl* ACL the first time you set any service profile's **auth-fallthru** option to **web-portal**.)

Mode

Enabled.

Usage

The first time you set the service profile's **auth-fallthru** option to **web-portal**, MSS sets the **web-portal-acl** option to *portalacl*. The value remains *portalacl* even if you change the **auth-fallthru** option again. To change the **web-portal-acl** value, you must use the **set service-profile web-portal-acl** command.

The Web-Portal ACL applies only to users who log on using Web-Portal, and applies only during authentication. After a Web-Portal user is authenticated, the Web-Portal ACL no longer applies. ACLs and other user attributes assigned to the username are applied instead.

Example

The following command changes the Web-Portal ACL name to on service profile *sp3* to *creditsrvr*:

```
RBT-8100# set service-profile sp3 web-portal-acl creditsrvr
success: change accepted.
```

Related Commands

- set service-profile auth-fallthru on page 11-82
- show service-profile on page 11-160

set service-profile web-portal-form

Specifies a custom login page to serve to WebAAA users who request the SSID managed by the service profile.

Syntax

set service-profile *name* **web-portal-form** *url*

Parameters

name	Service profile name.
url	RoamAbout switch subdirectory name and HTML page name of the login page. Specify the full path. For example, *corpa-ssid/corpa.html*.

Defaults

The Enterasys Networks Web login page is served by default.

Mode

Enabled.

Usage

Enterasys Networks recommends that you create a subdirectory for the custom page and place all the page's files in that subdirectory. Do not place the custom page in the root directory of the switch's user file area.

If the custom login page includes gif or jpg images, their path names are interpreted relative to the directory from which the page is served.

Note: To use WebAAA, the fallthru authentication type in the service profile that manages the SSID must be set to **web-portal**. To use WebAAA for a wired authentication port, edit the port configuration with the **set port type wired-auth** command.

The **web-portal** authentication type also requires additional configuration items. (See the "Configuring AAA for Network Users" chapter of the *RoamAbout Mobility System Software Configuration Guide*.)

Example

The following commands create a subdirectory named *corpa*, copy a custom login page named *corpa-login.html* and a jpg image named *corpa-logo.jpg* into that subdirectory, and set the Web login page for service profile *corpa-service* to *corpa-login.html*:

```
RBT-8100# mkdir corpa
success: change accepted.
RBT-8100# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
RBT-8100# copy tftp://10.1.1.1/corpa-logo.jpg corpa/corpa-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]
RBT-8100# dir corpa
================================================================================
file:
Filename                                        Size           Created
file:corpa-login.html                          637 bytes   Aug 12 2004, 15:42:26
file:corpa-logo.jpg                           1202 bytes   Aug 12 2004, 15:57:11
Total:        1839 bytes used, 206577 Kbytes free
RBT-8100# set service-profile corpa-service web-portal-form corpa/corpa-
login.html
success: change accepted.
```

Related Commands

- copy on page 20-5
- dir on page 20-8
- mkdir on page 20-14
- set port type wired-auth on page 4-26
- set service-profile auth-fallthru on page 11-82
- set web-portal on page 8-61
- show service-profile on page 11-160

set service-profile web-portal-session-timeout

Changes the number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically.

Syntax

set service-profile *name* **web-portal-session-timeout** *seconds*

Parameters

name	Service profile name.
seconds	Number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically. You can specify from 5 to 2800 seconds.

Defaults

The default Web Portal WebAAA session timeout is 5 seconds.

Mode

Enabled.

Usage

When a client that has connected through Web Portal WebAAA enters standby or hibernation mode, the client may be idle for longer than the User idle-timeout period. When the User idle-timeout period expires, MSS places the client's Web Portal WebAAA session in the Deassociated state. The Web Portal WebAAA session can remain in the Deassociated state for a configurable amount of time before being terminated automatically. This configurable amount of time is called the Web Portal WebAAA session timeout period. You can use this command to set the number of seconds in the Web Portal WebAAA session timeout period.

Note: The Web Portal WebAAA session timeout period applies only to Web Portal WebAAA sessions already authenticated with a username and password. For all other Web Portal WebAAA sessions, the default Web Portal WebAAA session timeout period of 5 seconds is used.

Example

The following command allows Web Portal WebAAA sessions to remain in the Deassociated state 180 seconds before being terminated automatically.

```
RBT-8100# set service-profile sp1 web-portal-session-timeout 180
success: change accepted.
```

Related Commands

- set service-profile user-idle-timeout on page 11-119
- show service-profile on page 11-160

set service-profile wep active-multicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting multicast frames.

Syntax

set service-profile *name* **wep active-multicast-index** *num*

Parameters

name	Service profile name.
num	WEP key number. You can enter a value from 1 through 4.

Defaults

If WEP encryption is enabled and WEP keys are defined, access point radios use WEP key 1 to encrypt multicast frames, by default.

Mode

Enabled.

Usage

Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Example

The following command configures service profile *sp2* to use WEP key 2 for encrypting multicast traffic:

```
RBT-8100# set service-profile sp2 wep active-multicast-index 2
success: change accepted.
```

Related Commands

- set service-profile wep active-unicast-index on page 11-125
- set service-profile wep key-index on page 11-126
- show service-profile on page 11-160

set service-profile wep active-unicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting unicast frames.

Syntax

set service-profile *name* **wep active-unicast-index** *num*

Parameters

name	Service profile name.
num	WEP key number. You can enter a value from 1 through 4.

Defaults

If WEP encryption is enabled and WEP keys are defined, access point radios use WEP key 1 to encrypt unicast frames, by default.

Mode

Enabled.

Usage

Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Example

The following command configures service profile *sp2* to use WEP key 4 for encrypting unicast traffic:

```
RBT-8100# set service-profile sp2 wep active-unicast-index 4
success: change accepted.
```

Related Commands

- set service-profile wep active-multicast-index on page 11-124
- set service-profile wep key-index on page 11-126
- show service-profile on page 11-160

set service-profile wep key-index

Sets the value of one of four static Wired-Equivalent Privacy (WEP) keys for static WEP encryption.

Syntax

set service-profile *name* **wep key-index** *num* **key** *value*

Parameters

name	Service profile name.
key-index *num*	WEP key index. You can enter a value from 1 through 4.
key *value*	Hexadecimal value of the key. You can enter a 10-character ASCII string representing a 5-byte hexadecimal number or a 26-character ASCII string representing a 13-byte hexadecimal number. You can use numbers or letters. ASCII characters in the following ranges are supported: • 0 to 9 • A to F • a to f

Defaults

By default, no static WEP keys are defined.

Mode

Enabled.

Usage

MSS automatically enables static WEP when you define a WEP key. MSS continues to support dynamic WEP.

Example

The following command configures a 5-byte WEP key for key index 1 on service profile *sp2* to *aabbccddee*.

```
RBT-8100# set service-profile sp2 wep key-index 1 key aabbccddee
success: change accepted.
```

Related Commands

- set service-profile wep active-multicast-index on page 11-124
- set service-profile wep active-unicast-index on page 11-125
- show service-profile on page 11-160

set service-profile wpa-ie

Enables the WPA information element (IE) in wireless frames. The WPA IE advertises the WPA authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax

set service-profile *name* **wpa-ie** {**enable** | **disable**}

Parameters

name	Service profile name.
enable	Enables the WPA IE.
disable	Disables the WPA IE.

Defaults

The WPA IE is disabled by default.

Mode

Enabled.

Usage

When the WPA IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

Example

The following command enables the WPA IE in service profile *sp2*:

```
RBT-8100# set service-profile sp2 wpa-ie enable
success: change accepted.
```

Related Commands

- set service-profile auth-dot1x on page 11-80
- set service-profile auth-psk on page 11-84
- set service-profile cipher-ccmp on page 11-88
- set service-profile cipher-tkip on page 11-89
- set service-profile cipher-wep104 on page 11-90
- set service-profile cipher-wep40 on page 11-91
- show service-profile on page 11-160

show {ap | dap} config

Displays global and radio-specific settings for an access point.

Syntax

show ap config [*port-list* [**radio** {**1** | **2**}]
show dap config [*dap-num* [**radio** {**1** | **2**}]]

Parameters

port-list	List of ports connected to the access point(s) for which to display configuration settings.
dap-num	Number of a Distributed access point for which to display configuration settings.
radio 1	Shows configuration information for radio 1.
radio 2	Shows configuration information for radio 2. (This option does not apply to single-radio models.)

Defaults

None.

Mode

Enabled.

Usage

MSS lists information separately for each access point.

Examples

The following example shows configuration information for an access point on RoamAbout switch port 2:

```
RBT-8100# show ap config 2
Port  2: AP model: RBT-1602, POE:  enable, bias: high, name: AP02
           boot-download-enable: YES
           force-image-download:  NO
           load balancing group: none
           location: The conference room
           contact: Bob the IT guy
  Radio 1: type: 802.11g, mode: disabled, channel:  6
  tx pwr:  1, profile: default
auto-tune max-power: default
  Radio 2: type: 802.11a, mode: disabled, channel: 36
  tx pwr:  1, profile: default
  auto-tune max-power: default
```

The following example shows configuration information for a Distributed access point configured on connection 1:

```
RBT-8100# show dap config 1
Dap  1: serial-id:   12345678, AP model: RBT-1602, bias: high, name: DAP01
        fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
        boot-download-enable: YES
        force-image-download:  NO
        load balancing group: none
        location: The conference room
           contact: Bob the IT guy
Radio 1: type: 802.11g, mode: disabled, channel:  6
  tx pwr:  1, profile: default
  auto-tune max-power: default
  Radio 2: type: 802.11a, mode: disabled, channel: 36
  tx pwr:  1, profile: default
  auto-tune max-power: default
```

Table 11-6 describes the fields in this display.

Table 11-6 Output for show ap config

Output	What it displays...
force-image-download	State of the option to force the AP to to download its software image from the RoamAbout Switch instead of loading the image that is locally stored on the AP.”.
Port	RoamAbout switch port number. **Note:** This field is applicable only if the AP is directly connected to the RoamAbout switch and the RoamAbout switch’s port is configured as an AP access port.
DAP	Connection ID for the Distributed access point. **Note:** This field is applicable only if the access point is configured on the RoamAbout switch as a Distributed access point.
serial-id	Serial ID of the access point. **Note:** This field is displayed only for Distributed access points.
AP model	Access point model number.
POE	PoE state on the RoamAbout switch port: • Enable • Disable
bias	Bias of the RoamAbout switch connection to the access point: • High • Low
name	Access point name.

Table 11-6 Output for show ap config (continued)

Output	What it displays...
fingerprint	Hexadecimal fingerprint of the access point's public encryption key. **Note:** This field is displayed only for Distributed access points. If the field is blank, the key has not been verified yet by an administrator. (See set dap fingerprint on page 11-26.)
boot-download-enable	State of the firmware upgrade option: • YES (automatic upgrades are enabled) • NO (automatic upgrades are disabled)
force-image-download	State of the option to force the AP to download its software image from the RoamAbout Switch instead of loading the image that is locally stored on the AP.
load balancing group	Names of the access point load-balancing groups to which the access point belongs. If the value is *None*, the access point does not belong to any load balancing groups. **Note:** This field is displayed only if the access point is a member of a group.
Radio	Radio number. The information listed below this field applies specifically to the radio.
type	Radio type: • 802.11a • 802.11b • 802.11g
mode	Radio state: • Enabled • Disabled
channel	Channel number.
antennatype	External antenna model, if applicable.
tx pwr	Transmit power, in dBm.
profile	Radio profile that manages the radio. Until you assign the radio to a radio profile, MSS assigns the radio to the default radio profile.
auto-tune max-power	Maximum power level the RF Auto-Tuning feature can set on the radio. • The value *default* means RF Auto-Tuning can set the power up to the maximum level allowed for the country of operation. • A specific numeric value means you or another administrator set the maximum value.

Related Commands

- set dap on page 4-15
- set {ap | dap} bias on page 11-18
- set dap fingerprint on page 11-26
- set {ap | dap} group on page 11-28

- set {ap | dap} name on page 11-30
- set {ap | dap} upgrade-firmware on page 11-44
- set {ap | dap} radio mode on page 11-38
- set {ap | dap} radio channel on page 11-35
- set {ap | dap} radio radio-profile on page 11-39
- set {ap | dap} radio tx-power on page 11-40
- show dap connection on page 11-151
- show dap global on page 11-153
- show dap unconfigured on page 11-155
- show radio-profile on page 11-157

show {ap | dap} counters

Displays access point and radio statistics counters.

Syntax

show ap counters [*port-list* [**radio** {**1** | **2**}]]
show dap counters [*dap-num* [**radio** {**1** | **2**}]]

Parameters

port-list	List of ports connected to the access point(s) for which to display statistics counters.
dap-num	Number of a Distributed access point for which to display statistics counters.
radio 1	Shows statistics counters for radio 1.
radio 2	Shows statistics counters for radio 2. (This option does not apply to single-radio models.)

Defaults

None.

Mode

Enabled.

Usage

To display statistics counters and other information for individual user sessions, use the **show sessions network** command.

Example

The following command shows statistics counters for an access point on port 7:

```
RBT-8100# show ap counters 7
Port: 7                radio: 1
================================
LastPktXferRate        2         PktTxCount         91594255
NumCntInPwrSave        4294966683MultiPktDrop       0
LastPktRxSigStrength   -54       MultiBytDrop       0
LastPktSigNoiseRatio   40        User Sessions      5
TKIP Pkt Transfer Ct   0         MIC Error Ct       0
TKIP Pkt Replays       0         TKIP Decrypt Err   0
CCMP Pkt Decrypt Err   0         CCMP Pkt Replays   0
CCMP Pkt Transfer Ct   0         RadioResets        0

     TxUniPkt     TxUniByte        RxPkt  RxByte   UndcrptPkt
            TxMultiPkt     TxMultiByte                  UndcrptByte
                                                             PhyError
 1.0: 164492     0  9631741       0 405041  8913512    0     0 13963
```

```
 2.0:    603     0   248716       0 191103  4608065    0    0 30547
 5.5: 370594 52742 27616521 4445625   2427   133217    0    0   723
11.0:   8016     0  2590353       0  85479  3897587    0    0  1195
TOTL: 543705 52742 40087331 4445625 684050 17552381    0    0 46441

Port: 7               radio: 2
================================
LastPktXferRate       24        PktTxCount         374415
NumCntInPwrSave       616       MultiPktDrop       0
LastPktRxSigStrength  -80       MultiBytDrop       0
LastPktSigNoiseRatio  6         User Sessions      0
TKIP Pkt Transfer Ct  0         MIC Error Ct       0
TKIP Pkt Replays      0         TKIP Decrypt Err   0
CCMP Pkt Decrypt Err  0         CCMP Pkt Replays   0
CCMP Pkt Transfer Ct  0         RadioResets        0

     TxUniPkt    TxUniByte       RxPkt  RxByte  UndcrptPkt
            TxMultiPkt    TxMultiByte               UndcrptByte
                                                         PhyError
 6.0:   1888     0   632537       0  89354 1947920    0    0    421
 9.0:    508     0   149925       0      0       0    0    0      0
12.0:     16     0      768       0      3     681    0    0      1
18.0:    240     0    80769       0      5    1017    0    0      0
24.0: 107057 7694  8085317 629107   1663   63543    0    0 141546
36.0:    453     0   132499       0    254   20533    0    0      1
48.0:   1152     0   601435       0   1303   65461    0    0     27
54.0:   5351     0  1960146       0  19533 1269084    0    0    904
TOTL: 116665 7694 11643396 629107 112115 3368239    0    0 142900
```

Table 11-7 describes the fields in this display.

Table 11-7 Output for show ap counters

Output	What it displays...
Port	RoamAbout switch port number.
radio	Radio number.
LastPktXferRate	Data transmit rate, in Mbps, of the last packet received by the access point.
NumCntInPwrSave	Number of clients currently in power save mode.
LastPktRxSigStrength	Signal strength, in dBm, of the last packet received by the access point.
LastPktSigNoiseRatio	Signal-to-noise ratio, in decibels (dB), of the last packet received by the access point.
TKIP Pkt Transfer Ct	Total number of TKIP packets sent and received by the radio.
TKIP Pkt Replays	Number of packets dropped because they were detected as TKIP replays. TKIP replays are packets received outside the TKIP sequence counter window.

Table 11-7 Output for show ap counters (continued)

Output	What it displays...
CCMP Pkt Decrypt Err	Number of times a decryption error occurred with a packet encrypted with CCMP.
CCMP Pkt Transfer Ct	Total number of CCMP packets sent and received by the radio.
PktTxCount	Number of packets transmitted by the radio.
MultiPktDrop	Number of multicast packets dropped by the radio.
MultiBytDrop	Number of multicast bytes dropped by the radio.
User Sessions	Number of users currently associated with the radio.
MIC Error Ct	Number of times the radio received a TKIP-encrypted frame with an invalid MIC.
TKIP Decrypt Err	Number of times a decryption error occurred with a packet encrypted with TKIP.
CCMP Pkt Replays	Number of packets dropped because they were detected as CCMP replays. CCMP replays are packets received outside the CCMP sequence counter window.
RadioResets	Number of times the radio has been reset.
TxUniPkt	Number of unicast packets transmitted by the radio. **Note:** This and the following statistics are listed separately for each data rate.
TxMultiPkt	Number of multicast packets transmitted by the radio.
TxUniByte	Number of unicast bytes transmitted by the radio.
TxMultiByte	Number of multicast bytes transmitted by the radio.
RxPkt	Number of packets received by the radio.
RxByte	Number of bytes received by the radio.
UndcrptPkt	Number of undecryptable packets received by the radio.
UndcrptByte	Number of undecryptable bytes received by the radio.
PhyError	Number of packets received by the radio that contained Physical layer (PHY) errors.

Related Commands

show sessions network on page 18-7

show {ap | dap} qos-stats

Displays statistics for access point forwarding queues.

Syntax

show dap qos-stats [*dap-num*] [**clear**]

show ap qos-stats [*port-list*] [**clear**]

Parameters

dap-num	Number of a Distributed access point for which to display QoS statistics counters.
port-list	List of ports connected to the access point(s) for which to display QoS statistics counters.
clear	Clears the counters after displaying their current values.

Defaults

None.

Mode

Enabled.

Usage

Repeating this command with the **clear** option at regular intervals allows you to monitor transmission and drop rates.

Example

The following command shows statistics for the access point forwarding queues on a Distributed access point:

```
RBT-8100# show dap qos-stats 4

CoS   Queue      Tx         TxDrop
=====================================
    DAP: 4 radio: 1
1,2   Background          0          0
0,3   BestEffort      15327        278
4,5   Video               0          0
6,7   Voice         1714881          0
    DAP: 4 radio: 2
1,2   Background          0          0
0,3   BestEffort          0          0
4,5   Video               0          0
6,7   Voice               0          0
```

Table 11-16 describes the fields in this display.

Table 11-8 Output for show {ap | dap} qos-stats

Output	What it displays...
CoS	CoS value associated with the forwarding queues.
Queue	Forwarding queue.
DAP or Port	Distributed access point number or access point port number.
radio	Radio number.
TxDrop	Number of packets dropped from the queue instead of being transmitted. Some packet drops are normal, especially if the RF environment is *noisy*. Also, it is normal for a mildly congested radio to drop low-priority packets proportionally more often than high-priority packets. However, continuous packet drops from the Voice queue can indicate over-subscription or excessive interference in the RF environment.
Tx	Number of packets transmitted to the air from the queue.

show {ap | dap} etherstats

Displays Ethernet statistics for an access point's Ethernet ports.

Syntax

show {**ap** | **dap**} **etherstats** [*port-list* | *dap-num*]

Parameters

port-list	List of RoamAbout switch ports directly connected to the access point(s) for which to display counters.
dap-num	Number of a Distributed access point for which to display counters.

Defaults

None.

Mode

Enabled.

Example

The following command displays Ethernet statistics for the Ethernet ports on Distributed access point 1:

```
RBT-8100# show dap etherstats 1
DAP: 1                ether: 1
================================
RxUnicast:          75432   TxGoodFrames:       55210
RxMulticast:        18789   TxSingleColl:          32
RxBroadcast:            8   TxLateColl:             0
RxGoodFrames:       94229   TxMaxColl:              0
RxAlignErrs:            0   TxMultiColl:           47
RxShortFrames:          0   TxUnderruns:            0
RxCrcErrors:            0   TxCarrierLoss:          0
RxOverruns:             0   TxDeferred:           150
RxDiscards:             0

DAP: 1                ether: 2
================================
RxUnicast:          64379   TxGoodFrames:       60621
RxMulticast:        21798   TxSingleColl:          32
RxBroadcast:           11   TxLateColl:             0
RxGoodFrames:       86188   TxMaxColl:              0
RxAlignErrs:            0   TxMultiColl:           12
RxShortFrames:          0   TxUnderruns:            0
RxCrcErrors:            0   TxCarrierLoss:          0
RxOverruns:             0   TxDeferred:           111
RxDiscards:             0
```

Table 11-9 describes the fields in this display.

Table 11-9 Output for show {ap | dap} etherstats

Output	What it displays...
RxUnicast	Number of unicast frames received.
RxMulticast	Number of multicast frames received.
RxBroadcast	Number of broadcast frames received.
RxGoodFrames	Number of frames received properly from the link.
RxAlignErrs	Number of received frames that were both misaligned and contained a CRC error.
RxShortFrames	Number of received frames that were shorter than the minimum frame length.
RxCrcErrors	Number of received frames that were discarded due to CRC errors.
RxOverruns	Number of frames known to be lost due to a temporary lack of hardware resources.
RxDiscards	Number of frames known to be lost due to a temporary lack of software resources.
TxGoodFrames	Number of frames transmitted properly on the link.
TxSingleColl	Number of transmitted frames that encountered a single collision.
TxLateColl	Number of frames that were not transmitted because they encountered a collision outside the normal collision window.
TxMaxColl	Number of frames that were not transmitted because they encountered the maximum allowed number of collisions. Typically, this occurs only during periods of heavy traffic on the network.
TxMultiColl	Number of transmitted frames that encountered more than one collision.
TxUnderruns	Number of frames that were not transmitted or retransmitted due to temporary lack of hardware resources.
TxCarrierLoss	Number of frames transmitted despite the detection of a deassertion of CRS during the transmission.
TxDeferred	Number of frames deferred before transmission due to activity on the link.

show {ap | dap} group

Displays configuration information and load-balancing status for access point groups.

Syntax

show {**ap** | **dap**} **group** [*name*]

Parameters

name	Name of an access point group or Distributed access point group.

Defaults

None.

Mode

Enabled.

Example

The following command displays information for access point group *loadbalance1*:

```
RBT-8100# show ap group loadbalance1

Load Balance Grp Port Clients   Status    Refused
---------------- ---- -------   --------- -------
    loadbalance1    1       1   Accepting       0
    loadbalance1    7       6   Refusing        2
```

Table 11-10 describes the fields in this display.

Table 11-10 Output for show ap group

Output	What it displays...
Load Balance Grp	Name of the access point group.
Port	RoamAbout switch port number.
Clients	Number of active client sessions on the access point.
Status	Association status of the access point: • Accepting—The access point is accepting new associations. • Refusing—The access point is refusing new associations.
Refused	Number of association requests refused by the access point due to load balancing. MSS resets this counter to 0 when the RoamAbout switch is restarted, MSS is reloaded, or the access point is removed from the group.

Related Commands

- set {ap | dap} group on page 11-28
- show {ap | dap} config on page 11-128

show {ap | dap} status

Displays access point and radio status information.

Syntax

show ap status [**terse**] | [*port-list* | **all** [**radio** {**1** | **2**}]]

show dap status [**terse**] | [*dap-num* | **all** [**radio** {**1** | **2**}]]

Parameters

terse	Displays a brief line of essential status information for each access point.
port-list	List of ports connected to the access point(s) for which to display status.
dap-num	Number of a Distributed access point for which to display status.
all	Shows status information for all Distributed access points configured on the switch.
radio 1	Shows status information for radio 1.
radio 2	Shows status information for radio 2. (This option does not apply to single-radio models.)

Defaults

None.

Mode

Enabled.

Examples

The following command displays the status of a Distributed access point:

```
RBT-8100# show dap status 1
Dap: 1, IP-addr: 10.2.30.5 (vlan 'vlan-corp'), AP model: AP3000,
        manufacturer: Enterasys, name: DAP01
        fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
==================================================
State:     operational (not encrypted)
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                id=0x29c15335347f1919 ram=33554432
                s/n=0333703027 hw_rev=A3
Uptime:    18 hours, 36 minutes, 27 seconds

Radio 1 type: 802.11g, state: configure succeed [Enabled] (802.11b protect)
      operational channel: 1 operational power: 14
      base mac: 00:0b:0e:00:d2:c0
      bssid1: 00:0b:0e:00:d2:c0, ssid: public
      bssid2: 00:0b:0e:00:d2:c2, ssid: employee-net
      bssid3: 00:0b:0e:00:d2:c4, ssid: mycorp-tkip
```

```
Radio 2 type: 802.11a, state: configure succeed [Enabled]
      operational channel: 64 operational power: 14
      base mac: 00:0b:0e:00:d2:c1
      bssid1: 00:0b:0e:00:d2:c1, ssid: public
      bssid2: 00:0b:0e:00:d2:c3, ssid: employee-net
      bssid3: 00:0b:0e:00:d2:c5, ssid: mycorp-tkip
      RFID Reports: Inactive
```

The following command uses the **terse** option to display brief information for Distributed access points:

```
RBT-8100# show dap status terse
Total number of entries: 4
Operational: 1, Image Downloading: 0, Unknown: 3, Other: 0
Flags: o = operational, b = booting, d = image downloading
       c = configuring, f = configuration failed
       a = auto DAP, i = insecure
Port   Flg IP Address      Model  MAC Address       Radio1 Radio2 Uptime
------ --- ------------- ------ ----------------- ------ ------ ------------
     3 ---               AP3000                   D ?/?  D ?/?   0d 0h 0m 0s
Dap  1 ---               AP3000                   D ?/?  D ?/?   0d 0h 0m 0s
Dap  2 ---               AP3000                   D ?/?  D ?/?   0d 0h 0m 0s
Dap100 oa- 10.8.255.11   AP3000 00:0b:0e:da:da:82 E 1/17 E36/11  0d 0h 0m17s
```

Table 11-11 and Table 11-11 describe the fields in these displays.

Table 11-11 Output for show ap status

Output	What it displays...
DAP	Connection ID for the Distributed access point. **Note:** This field is applicable only if the access point is configured on the RoamAbout switch as a Distributed access point.
Port	RoamAbout switch port number. **Note:** This field is applicable only if the access point is directly connected to the RoamAbout switch and the RoamAbout switch's port is configured as an AP access port.
IP-addr	IP address of the access point. The address is assigned to the access point by a DHCP server. **Note:** This field is applicable only if the access point is configured on the RoamAbout switch as a Distributed access point.
AP model	Access point access point model number.
manufacturer	Company that made the access point.
fingerprint	Hexadecimal fingerprint of the access point's public encryption key. **Note:** This field is displayed only for Distributed access points.
name	Access point name.
Link	Status of this link with the access point and the access point port at the other end of the link. The status can be up or down.

Table 11-11 Output for show ap status (continued)

Output	What it displays...
Access point port	Access point port number connected to this RoamAbout switch port.
State	State of the access point: • init—The access point has been recognized by the RoamAbout switch but has not yet begun booting. • booting—The access point has asked the RoamAbout switch for a boot image. • image downloading—The access point is receiving a boot image from the RoamAbout switch. • image downloaded—The access point has received a boot image from the RoamAbout switch and is booting. • configuring—The access point has booted and is ready to receive or is already receiving configuration parameters from the RoamAbout switch. • operational—The access point has received configuration parameters for one or more radios and is ready to accept client connections. • configure failure—One or more of the radio parameters received from the RoamAbout switch is invalid. For Distributed access points, this field also indicates whether the access point's management traffic with the RoamAbout switch is encrypted, and whether the access point's fingerprint has been verified on the RoamAbout switch: • not encrypted—The management session is not encrypted. • encrypted but fingerprint not verified—The access point's management traffic is encrypted, but the access point's fingerprint has not been verified in MSS. • encrypted and verified—The access point's management traffic is encrypted and the access point's fingerprint has been verified in MSS.
CPU info	Specifications and identification of the CPU.
Uptime	Amount of time since the access point booted using this link.

Table 11-11 Output for show ap status (continued)

Output	What it displays...

Radio 1 type
Radio 2 type
	802.11 type and configuration state of the radio.
	• The *configure succeed* state indicates that the access point has received configuration parameters for the radio and the radio is ready to accept client connections.
	• *802.11b protect* indicates that the 802.11b/g radio is sending messages to 802.11b devices, while sending 802.11g traffic at higher data rates, to inform the 802.11b devices about the 802.11g traffic and reserve bandwidth for the traffic. Protection mode remains in effect until 60 seconds after the last 802.11b traffic is detected by the 802.11b/g radio.
	• *Sweep Mode* indicates that a disabled radio is nonetheless participating in rogue detection scans. Even though this message appears only for disabled radios, all radios, enabled or disabled, participate in rogue detection.
	• *Countermeasures Enabled* indicates that the radio is sending countermeasures packets to combat a rogue.
	• *Radar Scan* indicates that the radio is performing the initial channel availability check for Dynamic Frequency Selection (DFS). This state lasts during the first 60 seconds an 802.11a radio is on a new channel, during which time the radio does not transmit. If the radio does not detect any radar on the channel, the radio starts using the channel for data. If the radio does detect radar, the flag changes to *Radar Detected*. (See below).
	• *Radar Detected* indicates that DFS has detected radar on the channel. When this occurs, the AP stops transmitting on the channel for 30 minutes. If RF Auto-Tuning is enabled for channel assignment, the radio selects another channel and performs the initial channel availability check on the new channel, during which time the flag changes back to *Radar Scan*.
	• The following information appears for external antennas:
	  • *External antenna detected, configured as* ***antenna-model***—Indicates that an external antenna has been detected, and lists the antenna model configured on the radio. (MSS does not detect the specific model.)
	  • *External antenna detected, not configured*—Indicates that an external antenna was detected but no external antenna is configured on the radio.
	  • *External antenna not detected, configured as* ***antenna-model***— Indicates that an external antenna is configured on the radio but no external antenna was detected.

operational channel	The channel on which the radio is currently operating. **Note:** If the channel number is followed by *(Auto)*, the value was set by RF Auto-Tuning.
operational power	The power level at which the radio is currently operating. **Note:** If the power setting is followed by *(Auto)*, the value was set by RF Auto-Tuning.
base mac	Base MAC address of the radio.
bssid, ssid	SSIDs configured on the radio and their BSSIDs.

Table 11-11 Output for show ap status (continued)

Output	What it displays...
RFID Reports	Status of AeroScout asset tag support. • Active—The AeroScout Engine has enabled the tag report mode on the AP. • Inactive—The AeroScout Engine has not enabled, or has disabled, the tag report mode on the AP. This field is displayed only if the **rfid-mode** option is enabled on the radio profile that manages the radio.

Table 11-12 Output for show ap status terse and show dap status terse

Output	What it displays...
Port	RoamAbout port number connected to the access point.
Flg	Operational status flags for the access point. For flag definitions, see the key in the command output.
IP Address	IP address of the access point. The address is assigned to the access point by a DHCP server. **Note:** This field is applicable only if the access point is configured on the RoamAbout switch as a Distributed access point.
Model	Access point model number.
MAC Address	MAC address of the access point.
Radio1	State, channel, and power information for radio 1: • The state can be D (disabled) or E (enabled). • The channel and power settings are shown as *channel*/*power*.
Radio2	State, channel, and power information for radio 2.
Uptime	Amount of time since the access point booted using this link.

show auto-tune attributes

Displays the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings.

Syntax

show auto-tune attributes [**ap** *AP-num* [**radio** {**1** | **2**| **all**}]]

show auto-tune attributes [**dap** *dap-num* [**radio** {**1** | **2**| **all**}]]

Parameters

ap-num	AP port connected to the access point for which to display RF attributes.
dap-num	Number of a Distributed access point for which to display RF attributes.
radio 1	Shows RF attribute information for radio 1.
radio 2	Shows RF attribute information for radio 2. (This option does not apply to single-radio models.)
radio all	Shows RF attribute information for both radios.

Defaults

None.

Mode

Enabled.

Example

The following command displays RF attribute information for radio 1 on the directly connected access point on port 2:

```
RBT-8100# show auto-tune attributes ap 2 radio 1
Auto-tune attributes for port 2 radio 1:
 Noise:                    -92 Packet Retransmission Count:          0
 Utilization:                0 Phy Errors Count:                     0
 CRC Errors count:       122
```

Table 11-13 describes the fields in this display.

Table 11-13 Output for show auto-tune attributes

Output	What it displays...
Noise	Noise threshold on the active channel. RF Auto-Tuning prefers channels with low noise levels over channels with higher noise levels.
Utilization	Number of multicast packets per second that a radio can send on a channel while continuously sending fixed size frames over a period of time. The number of packets that are successfully transmitted indicates how busy the channel is.

Table 11-13 Output for show auto-tune attributes (continued)

Output	What it displays...
CRC Errors count	Number of frames received by the radio on that active channel that had CRC errors. A high CRC error count can indicate a hidden node or co-channel interference.
Packet Retransmission Count	Number of retransmitted packets sent from the client to the radio on the active channel. Retransmissions can indicate that the client is not receiving ACKs from the access point radio.
Phy Errors Count	Number of frames received by the access point radio that had physical layer errors on the active channel. Phy errors can indicate interference from a non-802.11 device.

Related Commands

- set {ap | dap} radio auto-tune max-power on page 11-33
- set radio-profile auto-tune channel-config on page 11-46
- set radio-profile auto-tune channel-holddown on page 11-48
- set radio-profile auto-tune channel-interval on page 11-49
- set radio-profile auto-tune power-config on page 11-52
- set radio-profile auto-tune power-interval on page 11-53
- show auto-tune neighbors on page 11-147
- show radio-profile on page 11-157

show auto-tune neighbors

Displays the other Enterasys Networks radios and third-party 802.11 radios that an Enterasys radio can hear.

Syntax

```
show auto-tune neighbors [ap ap-num [radio {1 | 2| all}]]

show auto-tune neighbors [dap dap-num [radio {1 | 2| all}]]
```

Parameters

ap-num	access point port connected to the access point for which to display neighbors.
dap-num	Number of a Distributed access point for which to display neighbors.
radio 1	Shows neighbor information for radio 1.
radio 2	Shows neighbor information for radio 2. (This option does not apply to single-radio models.)
radio all	Shows neighbor information for both radios.

Defaults

None.

Mode

Enabled.

Usage

For simplicity, this command displays a single entry for each Enterasys radio, even if the radio is supporting multiple BSSIDs. However, BSSIDs for third-party 802.11 radios are listed separately, even if a radio is supporting more than one BSSID.

Information is displayed for a radio if the radio sends beacon frames or responds to probe requests. Even if a radio's SSIDs are unadvertised, Enterasys radios detect the empty beacon frames (beacon frames without SSIDs) sent by the radio, and include the radio in the neighbor list.

Example

The following command displays neighbor information for radio 1 on the directly connected access point on port 2:

```
RBT-8100# show auto-tune neighbors ap 2 radio 1
Total number of entries for port 2 radio 1: 5
Channel Neighbor BSS/MAC  RSSI
------- ----------------- ----
      1 00:0b:85:06:e3:60  -46
      1 00:0b:0e:00:0a:80  -78
      1 00:0b:0e:00:d2:c0  -74
      1 00:0b:85:06:dd:00  -50
      1 00:0b:0e:00:05:c1  -72
```

Table 11-11 describes the fields in this display.

Table 11-14 Output for show auto-tune neighbors

Field	Description
Channel	Channel on which the BSSID is detected.
Neighbor BSS/MAC	BSSID detected by the radio.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.

Related Commands

- set {ap | dap} radio auto-tune max-power on page 11-33
- set radio-profile auto-tune channel-config on page 11-46
- set radio-profile auto-tune channel-holddown on page 11-48
- set radio-profile auto-tune channel-interval on page 11-49
- set radio-profile auto-tune power-config on page 11-52
- set radio-profile auto-tune power-interval on page 11-53
- show auto-tune attributes on page 11-145
- show radio-profile on page 11-157

show dap boot-configuration

Displays information about the static IP address configuration (if any) on a Distributed AP.

Usage

show dap boot-configuration *dap-num*

Parameters

dap-num	Number of a Distributed AP for which to display static IP configuration information.

Defaults

None.

Mode

Enabled.

Example

The following command displays static IP configuration information for Distributed AP 1:

```
RBT-8100# show dap boot-configuration 1
Static Boot Configuration
DAP: 1

IP Address:  Disabled
VLAN Tag:    Disabled
Switch:             Disabled

IP Address:
Netmask:
Gateway:
VLAN Tag:
Switch IP:
Switch Name:
DNS IP:
```

Table 11-15 describes the fields in the example.

Table 11-15 Output for show dap boot-configuration

Field	Description
Flags	
DAP	Distributed AP number.
Enable ip	Whether static IP address assignment is enabled for this Distributed AP.
Enable vlan	Whether the Distributed AP is configured to use a VLAN tag.

Table 11-15 Output for show dap boot-configuration (continued)

Field	Description
Enable	Whether the Distributed AP is configured to use a manually specified RoamAbout Switch as its boot device.
Vlan Tag	The VLAN tag that the Distributed AP is configured to use (if any).
IP address	The static IP address assigned to this Distributed AP.
IP netmask	The subnet mask assigned to this Distributed AP.
gateway	The IP address of the default gateway assigned to this Distributed AP.
IP	The IP address of the RoamAbout Switch that this Distributed AP is configured to use as its boot device (if any).
DNS	The IP address of the DNS server that the Distributed AP uses to resolve the name of the RoamAbout Switch used as its boot device.

show dap connection

Displays the system IP address of the RoamAbout switch that booted a Distributed AP.

Syntax

show dap connection [*dap-num* | **serial-id** *serial-ID*]

Parameters

dap-num	Number of a Distributed access point for which to display information about its active connection.
serial-id *serial-ID*	Access point serial ID.

Defaults

None.

Mode

Enabled.

Usage

The **serial-id** parameter displays the active connection for the specified Distributed access point even if that access point is not configured on this RoamAbout switch. If you instead use the command with the *dap-num* parameter or without a parameter, connection information is displayed only for Distributed access points that are configured on this RoamAbout switch.

This command provides information only if the Distributed AP is configured on the switch where you use the command. The switch does not need to be the one tht booted the AP, but it must have the AP in its configuration. Also, the switch that booted the AP must be in the same Mobility Domain as the switch where you use the command.

If a Distributed AP is configured on this RoamAbout Switch (or another RoamAbout switch in the same Mobility Domain) but does not have an active connection, the command does not display information for the AP. To show connection information for Distributed APs, use the **show dap global** command on one of the switches where the APs are configured.

Examples

The following command displays information for all Distributed access points configured on this RoamAbout switch that have active connections:

```
RBT-8100# show dap connection
Total number of entries: 2
DAP Serial Id   DAP IP Address  RBT IP Address
--- ----------- --------------- ---------------
2   112233      10.10.2.27      10.3.8.111
4   0333000298  10.10.3.34      10.3.8.111
```

The following command displays connection information specifically for a Distributed access point with serial ID *223344*:

```
RBT-8100# show dap connection serial-id 223344
Total number of entries: 1
DAP Serial Id   DAP IP Address  RBT IP Address
--- ----------- --------------- ---------------
9   223344      10.10.4.88      10.9.9.11
```

Table 11-16 describes the fields in this display.

Table 11-16 Output for show dap connection

Field	Description
DAP	Connection ID you assigned to the Distributed access point. If the connection is configured on another RoamAbout switch, this field contains a hyphen (-).
Serial Id	Serial ID of the Distributed access point.
DAP IP Address	IP address assigned by DHCP to the Distributed access point.
RoamAbout IP Address	System IP address of the RoamAbout switch on which the access point has an active connection. This is the switch that the access point used for booting and configuration and is using for data transfer.

Related Commands

- show {ap | dap} config on page 11-128
- show dap global on page 11-153
- show dap unconfigured on page 11-155

show dap global

Displays connection information for Distributed APs configured on a RoamAbout switch.

Syntax

show dap global [*dap-num* | **serial-id** *serial-ID*]

Parameters

dap-num	Number of a Distributed access point for which to display configuration settings.
serial-id *serial-ID*	Access point serial ID.

Defaults

None.

Mode

Enabled.

Usage

To show information only for Distributed access points that have active connections, use the **show dap connection** command.

Example

The following command displays configuration information for all Distributed access points configured on a RoamAbout switch:

```
RBT-8100# show dap global
Total number of entries: 8
DAP Serial Id   RBT IP Address   Bias
--- ----------- --------------- ----
1   11223344    10.3.8.111      HIGH
-   11223344    10.4.3.2        LOW
2   332211      10.3.8.111      LOW
-   332211      10.4.3.2        HIGH
17  0322100185  10.3.8.111      HIGH
-   0322100185  10.4.3.2        LOW
18  0321500120  10.3.8.111      LOW
-   0321500120  10.4.3.2        HIGH
```

Table 11-17 describes the fields in this display.

Table 11-17 Output for show dap global

Field	Description
DAP	Connection ID you assigned to the Distributed access point. **Note:** DAP numbers are listed only for Distributed access points configured on this RoamAbout switch. If the field contains a hyphen (-), the Distributed access point configuration displayed in the row of output is on another RoamAbout switch.
Serial Id	Serial ID of the Distributed access point.
RoamAbout IP Address	System IP address of the RoamAbout switch on which the Distributed access point is configured. A separate row of output is displayed for each RoamAbout switch on which the Distributed access point is configured.
Bias	Bias of the RoamAbout switch for the Distributed access point: • High • Low

Related Commands

- set dap on page 4-15
- set {ap | dap} bias on page 11-18
- show {ap | dap} config on page 11-128
- show dap connection on page 11-151
- show dap unconfigured on page 11-155

show dap unconfigured

Displays Distributed access points that are physically connected to the network but that are not configured on any RoamAbout switches.

Syntax

show dap unconfigured

Defaults

None.

Mode

Enabled.

Usage

This command also displays an access point that is directly connected to a RoamAbout switch, if the RoamAbout port to which the access point is connected is configured as a network port instead of an access point access port, and if the network port is a member of a VLAN.

If a Distributed access point is configured on a RoamAbout switch in another Mobility Domain, the access point can appear in the output until the access point is able to establish a connection with a RoamAbout switch in its Mobility Domain. After the access point establishes a connection, the entry for the access point ages out and no longer appears in the command's output.

Entries in the command output's table age out after two minutes.

Example

The following command displays information for two Distributed access points that are not configured:

```
RBT-8100# show dap unconfigured
Total number of entries: 2
Serial Id   Model  IP Address      Port Vlan
----------- ------ --------------- ---- --------
0333001287  AP3000 10.3.8.54       5    default
0333001285  AP3000 10.3.8.57       7    vlan-eng
```

Table 11-18 describes the fields in this display.

Table 11-18 Output for show dap unconfigured

Field	Description
Serial Id	Serial ID of the Distributed access point.
Model	Access point model number.
IP Address	IP address of the access point. This is the address that the access point receives from a DHCP server. The access point uses this address to send a Find RoamAbout message to request configuration information from RoamAbout switches. However, the access point cannot use the address to establish a connection unless the access point first receives a configuration from a RoamAbout switch.

Table 11-18 Output for show dap unconfigured

Field	Description
Port	Port number on which this RoamAbout switch received the access point's Find RoamAbout message.
VLAN	VLAN on which this RoamAbout switch received the access point's Find RoamAbout message.

Related Commands

- show dap connection on page 11-151
- show dap global on page 11-153

show radio-profile

Displays radio profile information.

Syntax

show radio-profile {*name* | **?**}

Parameters

name	Displays information about the named radio profile.
?	Displays a list of radio profiles.

Defaults

None.

Mode

Enabled.

Usage

MSS contains a *default* radio profile. Enterasys Networks recommends that you do not change this profile but instead keep the profile for reference.

Example

The following command shows radio profile information for the *default* radio profile:

```
RBT-8100# show radio-profile default
Beacon Interval:                  100   DTIM Interval:                     1
Max Tx Lifetime:                 2000   Max Rx Lifetime:                2000
RTS Threshold:                   2346   Frag Threshold:                 2346
Long Preamble:                     no   Tune Channel:                     yes
Tune Power:                        no   Tune Channel Interval:          3600
Tune Power Interval:              600   Channel Holddown:                300
Power Backoff Timer:               10   Countermeasures:                none
Active-Scan:                      yes   QoS Mode:                        wmm

No service profiles configured.
```

Table 11-19 describes the fields in this display.

Table 11-19 Output for show radio-profile

Output	What it displays...
Beacon Interval	Rate (in milliseconds) at which each access point radio in the profile advertises the beaconed SSID.
DTIM Interval	Number of times after every beacon that each access point radio in the radio profile sends a delivery traffic indication map (DTIM).
Max Tx Lifetime	Number of milliseconds that a frame *received* by a radio in the radio profile can remain in buffer memory.

Table 11-19 Output for show radio-profile (continued)

Output	What it displays...
Max Rx Lifetime	Number of milliseconds that a frame *scheduled to be transmitted* by a radio in the radio profile can remain in buffer memory.
RTS Threshold	Minimum length (in bytes) a frame can be for a radio in the radio profile to use the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.
Frag Threshold	Maximum length (in bytes) a frame is allowed to be without being fragmented into multiple frames before transmission by a radio in the radio profile.
Long Preamble	Indicates whether an 802.11b radio that uses this radio profile advertises support for frames with long preambles only: • YES—Advertises support for long preambles only. • NO—Advertises support for long and short preambles.
Tune Channel	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning channels.
Tune Power	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning power levels.
Tune Channel Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.
Tune Power Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.
Client Backoff Timer	Interval, in minutes, at which radios in a radio profile reduce power after temporarily increasing the power to maintain the minimum data rate for an associated client. At the end of each power-backoff interval, radios that temporarily increased their power reduce it by 1 dBm. The power backoff continues in 1 dBm increments after each interval until the power returns to expected setting.
Channel Holddown	Minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel.
Countermeasures	Indicates whether countermeasures are enabled.
Active-Scan	Indicates whether the active-scan mode of RF detection is enabled.
QoS Mode	Indicates the Quality-of-Service setting for AP radio forwarding queues: • wmm—AP forwarding queues provide standard priority handling for WMM devices. • svp—SP forwarding queues are optimized for SpectraLink Voice Priority (SVP). For information about the QoS modes, see the “Configuring Quality of Service” chapter in the *RoamAbout Mobility System Software Configuration Guide*.

Table 11-19 Output for show radio-profile (continued)

Output	What it displays...
Service profiles	Service profiles mapped to this radio profile. Each service profile contains an SSID and encryption information for that SSID. **Note:** When you upgrade from 2.x, MSS creates a default-dot1x service profile for encrypted SSIDs and a default-clear service profile for unencrypted SSIDs. These default service profiles contain the default encryption settings for crypto SSIDs and clear SSIDs, respectively.

Related Commands

- set radio-profile auto-tune channel-config on page 11-46
- set radio-profile auto-tune channel-holddown on page 11-48
- set radio-profile auto-tune channel-interval on page 11-49
- set radio-profile auto-tune power-backoff-timer on page 11-51
- set radio-profile auto-tune power-config on page 11-52
- set radio-profile auto-tune power-interval on page 11-53
- set radio-profile beacon-interval on page 11-56
- set radio-profile dtim-interval on page 11-58
- set radio-profile frag-threshold on page 11-59
- set radio-profile max-rx-lifetime on page 11-61
- set radio-profile max-tx-lifetime on page 11-62
- set radio-profile mode on page 11-63
- set radio-profile preamble-length on page 11-66
- set radio-profile rts-threshold on page 11-69
- set radio-profile service-profile on page 11-70

show service-profile

Displays service profile information.

Syntax

show service-profile {*name* | **?**}

Parameters

name	Displays information about the named service profile.
?	Displays a list of service profiles.

Defaults

None.

Mode

Enabled.

Example

The following command displays information for service profile *wpa_clients*:

```
RBT-8100# show service-profile wpa_clients
ssid-name:         Enterasys ssid-type:          crypto
beacon:                yes    auth-fallthru:      web-portal
WEP Key 1 value:    <none>    WEP Key 2 value:    <none>
WEP Key 3 value:    <none>    WEP Key 4 value:    <none>
WEP Unicast Index:       1    WEP Multicast Index:     1
Shared Key Auth:        NO
WPA enabled:
    ciphers: cipher-tkip
    authentication: 802.1X
    TKIP countermeasures time: 60000ms
```

Table 11-20 describes the fields in this display.

Table 11-20 Output for show service-profile

Field	Description
ssid-name	Service set identifier (SSID) managed by this service profile.
ssid-type	SSID type: • crypto—Wireless traffic for the SSID is encrypted. • clear—Wireless traffic for the SSID is unencrypted.
beacon	Indicates whether the radio sends beacons, to advertise the SSID: • no • yes

Table 11-20 Output for show service-profile (continued)

Field	Description
auth-fallthru	Secondary (fallthru) encryption type when a user tries to authenticate but the RoamAbout switch managing the radio does not have an authentication rule with a userglob that matches the username. • last-resort—Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password. • none—Denies authentication and prohibits the user from accessing the SSID. • web-portal—Redirects the user to a web page for login to the SSID.
WEP Key 1 value	State of static WEP key number 1. Radios can use this key to encrypt traffic with static Wired-Equivalent Privacy (WEP): • none—The key is not configured. • preset—The key is configured. **Note:** The WEP parameters apply to traffic only on the encrypted SSID.
WEP Key 2 value	State of static WEP key number 2: • none—The key is not configured. • preset—The key is configured.
WEP Key 3 value	State of static WEP key number 3: • none—The key is not configured. • preset—The key is configured.
WEP Key 4 value	State of static WEP key number 4: • none—The key is not configured. • preset—The key is configured.
WEP Unicast Index	Index of the static WEP key used to encrypt unicast traffic on an encrypted SSID.
WEP Multicast Index	Index of the static WEP key used to encrypt multicast traffic on an encrypted SSID.
Shared Key Auth	Indicates whether shared-key authentication is enabled.

WPA enabled	Indicates that the Wi-Fi Protected Access (WPA) information element (IE) is enabled. Additional fields display the settings of other WPA parameters:
	• ciphers—Lists the WPA cipher suites advertised by radios in the radio profile mapped to this service profile.
	• authentication—Lists the authentication methods supported for WPA clients:
	  • 802.1X—dynamic authentication
	  • PSK—preshared key authentication
	• TKIP countermeasures time—Indicates the amount of time (in ms) MSS enforces countermeasures following a second message integrity code (MIC) failure within a 60-second period.
	Note: The WPA fields are displayed only when the WPA IE is enabled.

Related Commands

- set service-profile attr on page 11-78
- set service-profile auth-dot1x on page 11-80
- set service-profile auth-fallthru on page 11-82
- set service-profile auth-psk on page 11-84
- set service-profile beacon on page 11-85
- set service-profile cac-mode on page 11-86
- set service-profile cac-session on page 11-87
- set service-profile cipher-ccmp on page 11-88
- set service-profile cipher-tkip on page 11-89
- set service-profile cipher-wep104 on page 11-90
- set service-profile cipher-wep40 on page 11-91
- set service-profile cos on page 11-92
- set service-profile dhcp-restrict on page 11-93
- set service-profile idle-client-probing on page 11-94
- set service-profile long-retry-count on page 11-96
- set service-profile no-broadcast on page 11-97
- set service-profile proxy-arp on page 11-99
- set service-profile psk-phrase on page 11-100
- set service-profile psk-raw on page 11-101
- set service-profile rsn-ie on page 11-102
- set service-profile shared-key-auth on page 11-103
- set service-profile short-retry-count on page 11-104
- set service-profile soda mode on page 11-110
- set service-profile ssid-name on page 11-113
- set service-profile ssid-type on page 11-114
- set service-profile static-cos on page 11-115
- set service-profile tkip-mc-time on page 11-116
- set service-profile transmit-rates on page 11-117
- set service-profile user-idle-timeout on page 11-119
- set service-profile web-portal-form on page 11-121
- set service-profile web-portal-session-timeout on page 11-123
- set service-profile wep active-multicast-index on page 11-124
- set service-profile wep active-unicast-index on page 11-125

- set service-profile wep key-index on page 11-126
- set service-profile wpa-ie on page 11-127

12

STP Commands

Use Spanning Tree Protocol (STP) commands to configure and manage spanning trees on the virtual LANs (VLANs) configured on a RoamAbout switch, to maintain a loop-free network. This chapter presents STP commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear spantree portcost	12-2
clear spantree portpri	12-3
clear spantree portvlancost	12-4
clear spantree portvlanpri	12-5
clear spantree statistics	12-6
set spantree	12-7
set spantree backbonefast	12-8
set spantree fwddelay	12-9
set spantree hello	12-10
set spantree maxage	12-11
set spantree portcost	12-12
set spantree portfast	12-14
set spantree portpri	12-15
set spantree portvlancost	12-16
set spantree portvlanpri	12-17
set spantree priority	12-18
set spantree uplinkfast	12-19
show spantree	12-20
show spantree backbonefast	12-23
show spantree blockedports	12-24
show spantree portfast	12-25
show spantree portvlancost	12-27
show spantree statistics	12-28
show spantree uplinkfast	12-33

clear spantree portcost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge in all VLANs on a RoamAbout switch.

Syntax

clear spantree portcost *port-list*

Parameters

port-list	List of ports. The port cost is reset on the specified ports.

Defaults

None.

Mode

Enabled.

Usage

This command resets the cost in all VLANs. To reset the cost for only specific VLANs, use the **clear spantree portvlancost** command.

Example

The following command resets the STP port cost on ports 5 and 6 to the default value:

```
RBT-8100# clear spantree portcost 5-6
success: change accepted.
```

Related Commands

- clear spantree portvlancost on page 12-4
- set spantree portcost on page 12-12
- set spantree portvlancost on page 12-16
- show spantree on page 12-20
- show spantree portvlancost on page 12-27

clear spantree portpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge in all VLANs on a RoamAbout switch.

Syntax

clear spantree portpri *port-list*

Parameters

port-list	List of ports. The port priority is reset to 32 (the default) on the specified ports.

Defaults

None.

Mode

Enabled.

Usage

This command resets the priority in all VLANs. To reset the priority for only specific VLANs, use the **clear spantree portvlanpri** command.

Example

The following command resets the STP priority on port 9 to the default:

```
RBT-8100# clear spantree portpri 9
success: change accepted.
```

Related Commands

- clear spantree portvlanpri on page 12-5
- set spantree portpri on page 12-15
- set spantree portvlanpri on page 12-17
- show spantree on page 12-20

clear spantree portvlancost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a RoamAbout switch, or for all VLANs.

Syntax

clear spantree portvlancost *port-list* {**all** | **vlan** *vlan-id*}

Parameters

port-list	List of ports. The port cost is reset on the specified ports.
all	Resets the cost for all VLANs.
vlan *vlan-id*	VLAN name or number. MSS resets the cost for only the specified VLAN.

Defaults

None.

Mode

Enabled.

Usage

MSS does not change a port's cost for VLANs other than the one(s) you specify.

Example

The following command resets the STP cost for port 12 in VLAN *sunflower*:

```
RBT-8100# clear spantree portvlancost 12 vlan sunflower
success: change accepted.
```

Related Commands

- clear spantree portcost on page 12-2
- set spantree portcost on page 12-12
- set spantree portvlancost on page 12-16
- show spantree on page 12-20
- show spantree portvlancost on page 12-27

clear spantree portvlanpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

Syntax

clear spantree portvlanpri *port-list* {**all** | **vlan** *vlan-id*}

Parameters

port-list	List of ports. The port priority is reset to 32 (the default) on the specified ports.
all	Resets the priority for all VLANs.
vlan *vlan-id*	VLAN name or number. MSS resets the priority for only the specified VLAN.

Defaults

None.

Mode

Enabled.

Usage

MSS does not change a port's priority for VLANs other than the one(s) you specify.

Example

The following command resets the STP priority for port 20 in VLAN *avocado*:

```
RBT-8100# clear spantree portvlanpri 20 vlan avocado
success: change accepted.
```

Related Commands

- clear spantree portpri on page 12-3
- set spantree portpri on page 12-15
- set spantree portvlanpri on page 12-17
- show spantree on page 12-20

clear spantree statistics

Clears STP statistics counters for a network port or ports and resets them to 0.

Syntax

clear spantree statistics *port-list* [**vlan** *vlan-id*]

Parameters

port-list	List of ports. Statistics counters are reset on the specified ports.
vlan *vlan-id*	VLAN name or number. MSS resets statistics counters for only the specified VLAN.

Defaults

None.

Mode

Enabled.

Example

The following command clears STP statistics counters for ports 5, 11, and 19 through 22, for all VLANs:

```
RBT-8100# clear spantree statistics 5,11,19-22
success: change accepted.
```

Related Commands

show spantree statistics on page 12-28

set spantree

Enables or disables STP on one VLAN or all VLANs configured on a RoamAbout switch.

Syntax

set spantree {**enable** | **disable**} [{**all** | **vlan** *vlan-id* | **port** *port-list vlan-id*}]

Parameters

enable	Enables STP.
disable	Disables STP.
all	Enables or disables STP on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS enables or disables STP on only the specified VLAN, on all ports within the VLAN.
port *port-list vlan-id*	Port number or list and the VLAN the ports are in. MSS enables or disables STP on only the specified ports, within the specified VLAN.

Defaults

Disabled.

Mode

Enabled.

Examples

The following command enables STP on all VLANs configured on a RoamAbout switch:

```
RBT-8100# set spantree enable
success: change accepted.
```

The following command disables STP on VLAN *burgundy*:

```
RBT-8100# set spantree disable vlan burgundy
success: change accepted.
```

Related Commands

show spantree on page 12-20

set spantree backbonefast

Enables or disables STP backbone fast convergence on a RoamAbout switch. This feature accelerates a port's recovery following the failure of an indirect link.

Syntax

set spantree backbonefast {**enable** | **disable**}

Parameters

enable	Enables backbone fast convergence.
disable	Disables backbone fast convergence.

Defaults

STP backbone fast path convergence is disabled by default.

Mode

Enabled.

Usage

If you plan to use the backbone fast convergence feature, you must enable it on all the bridges in the spanning tree.

Example

The following command enables backbone fast convergence:

```
RBT-8100# set spantree backbonefast enable
success: change accepted.
```

Related Commands

show spantree backbonefast on page 12-23

set spantree fwddelay

Changes the period of time after a topology change that a RoamAbout switch which is not the root bridge waits to begin forwarding Layer 2 traffic on one or all of its configured VLANs. (The root bridge always forwards traffic.)

Syntax

set spantree fwddelay *delay* {**all** | **vlan** *vlan-id*}

Parameters

delay	Delay value. You can specify from 4 through 30 seconds.
all	Changes the forwarding delay on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the forwarding delay on only the specified VLAN.

Defaults

The default forwarding delay is 15 seconds.

Mode

Enabled.

Example

The following command changes the forwarding delay on VLAN *pink* to 20 seconds:

```
RBT-8100# set spantree fwddelay 20 vlan pink
success: change accepted.
```

Related Commands

show spantree on page 12-20

set spantree hello

Changes the interval between STP hello messages sent by a RoamAbout switch when operating as the root bridge, on one or all of its configured VLANs.

Syntax

set spantree hello *interval* {**all** | **vlan** *vlan-id*}

Parameters

interval	Interval value. You can specify from 1 through 10 seconds.
all	Changes the interval on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the interval on only the specified VLAN.

Defaults

The default hello timer interval is 2 seconds.

Mode

Enabled.

Example

The following command changes the hello interval for all VLANs to 4 seconds:

```
RBT-8100# set spantree hello 4 all
success: change accepted.
```

Related Commands

show spantree on page 12-20

set spantree maxage

Changes the maximum age for an STP root bridge hello packet that is acceptable to a RoamAbout switch acting as a designated bridge on one or all of its VLANs. After waiting this period of time for a new hello packet, the switch determines that the root bridge is unavailable and issues a topology change message.

Syntax

set spantree maxage *aging-time* {**all** | **vlan** *vlan-id*}

Parameters

aging-time	Maximum age value. You can specify from 6 through 40 seconds.
all	Changes the maximum age on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the maximum age on only the specified VLAN.

Defaults

The default maximum age for root bridge hello packets is 20 seconds.

Mode

Enabled.

Example

The following command changes the maximum acceptable age for root bridge hello packets on all VLANs to 15 seconds:

```
RBT-8100# set spantree maxage 15 all
success: change accepted.
```

Related Commands

show spantree on page 12-20

set spantree portcost

Changes the cost that transmission through a network port or ports in the default VLAN on a RoamAbout switch adds to the total cost of a path to the STP root bridge.

Syntax

set spantree portcost *port-list* **cost** *cost*

Parameters

port-list	List of ports. MSS applies the cost change to all the specified ports.
cost *cost*	Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.

Defaults

The default port cost depends on the port speed and link type. Table 12-1 lists the defaults for STP port path cost.

Table 12-1 SNMP Port Path Cost Defaults

Port Speed	Link Type	Default Port Path Cost
1000 Mbps	Full Duplex Aggregate Link (Port Group)	19
1000 Mbps	Full Duplex	4
100 Mbps	Full Duplex Aggregate Link (Port Group)	19
100 Mbps	Full Duplex	18
100 Mbps	Half Duplex	19
10 Mbps	Full Duplex Aggregate Link (Port Group)	19
10 Mbps	Full Duplex	95
10 Mbps	Half Duplex	100

Mode

Enabled.

Usage

This command applies only to the default VLAN (VLAN 1). To change the cost of a port in another VLAN, use the **set spantree portvlancost** command.

Example

The following command changes the cost on ports 3 and 4 to 20:

```
RBT-8100# set spantree portcost 3,4 cost 20
success: change accepted.
```

Related Commands

- clear spantree portcost on page 12-2
- clear spantree portvlancost on page 12-4
- set spantree portvlancost on page 12-16
- show spantree on page 12-20
- show spantree portvlancost on page 12-27

set spantree portfast

Enables or disables STP port fast convergence on one or more ports on a RoamAbout switch.

Syntax

set spantree portfast port *port-list* {**enable** | **disable**}

Parameters

port *port-list*	List of ports. MSS enables the feature on the specified ports.
enable	Enables port fast convergence.
disable	Disables port fast convergence.

Defaults

STP port fast convergence is disabled by default.

Mode

Enabled.

Usage

Use port fast convergence on ports that are directly connected to servers, hosts, or other MAC stations.

Example

The following command enables port fast convergence on ports 9, 11, and 13:

```
RBT-8100# set spantree portfast port 9,11,13 enable
success: change accepted.
```

Related Commands

show spantree portfast on page 12-25

set spantree portpri

Changes the STP priority of a network port or ports for selection as part of the path to the STP root bridge in the default VLAN on a RoamAbout switch.

Syntax

set spantree portpri *port-list* **priority** *value*

Parameters

port-list	List of ports. MSS changes the priority on the specified ports.
priority *value*	Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).

Defaults

The default STP priority for all network ports is 128.

Mode

Enabled.

Usage

This command applies only to the default VLAN (VLAN 1). To change the priority of a port in another VLAN, use the **set spantree portvlanpri** command.

Example

The following command sets the priority of ports 3 and 4 to 48:

```
RBT-8100# set spantree portpri 3-4 priority 48
success: change accepted.
```

Related Commands

- clear spantree portpri on page 12-3
- clear spantree portvlanpri on page 12-5
- set spantree portvlanpri on page 12-17
- show spantree on page 12-20

set spantree portvlancost

Changes the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a RoamAbout switch.

Syntax

set spantree portvlancost *port-list* **cost** *cost* {**all** | **vlan** *vlan-id*}

Parameters

port-list	List of ports. MSS applies the cost change to all the specified ports.
cost *cost*	Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.
all	Changes the cost on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the cost on only the specified VLAN.

Defaults

The default port cost depends on the port speed and link type. (See Table 12-1 on page 12.)

Mode

Enabled.

Example

The following command changes the cost on ports 3 and 4 to 20 in VLAN *mauve*:

```
RBT-8100# set spantree portvlancost 3,4 cost 20 vlan mauve
success: change accepted.
```

Related Commands

- clear spantree portcost on page 12-2
- clear spantree portvlancost on page 12-4
- set spantree portcost on page 12-12
- show spantree on page 12-20
- show spantree portvlancost on page 12-27

set spantree portvlanpri

Changes the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

Syntax

set spantree portvlanpri *port-list* **priority** *value* {**all** | **vlan** *vlan-id*}

Parameters

port-list	List of ports. MSS changes the priority on the specified ports.
priority *value*	Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).
all	Changes the priority on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the priority on only the specified VLAN.

Defaults

The default STP priority for all network ports is 128.

Mode

Enabled.

Example

The following command sets the priority of ports 3 and 4 to 48 on VLAN *mauve*:

```
RBT-8100# set spantree portvlanpri 3-4 priority 48 vlan mauve
success: change accepted.
```

Related Commands

- clear spantree portpri on page 12-3
- clear spantree portvlanpri on page 12-5
- set spantree portpri on page 12-15
- show spantree on page 12-20

set spantree priority

Changes the STP root bridge priority of a RoamAbout switch on one or all of its VLANs.

Syntax

set spantree priority *value* {**all** | **vlan** *vlan-id*}

Parameters

priority *value*	Priority value. You can specify a value from 0 through 65,535. The bridge with the lowest priority value is elected to be the root bridge for the spanning tree.
all	Changes the bridge priority on all VLANs.
vlan *vlan-id*	VLAN name or number. MSS changes the bridge priority on only the specified VLAN.

Defaults

The default root bridge priority for the switch on all VLANs is 32,768.

Mode

Enabled.

Example

The following command sets the bridge priority of VLAN *pink* to 69:

```
RBT-8100# set spantree priority 69 vlan pink
success: change accepted.
```

Related Commands

show spantree on page 12-20

set spantree uplinkfast

Enables or disables STP uplink fast convergence on a RoamAbout switch. This feature enables a RoamAbout switch with redundant links to the network backbone to immediately switch to the backup link to the root bridge if the primary link fails.

Syntax

set spantree uplinkfast {**enable** | **disable**}

Parameters

enable	Enables uplink fast convergence.
disable	Disables uplink fast convergence.

Defaults

Disabled.

Mode

Enabled.

Usage

The uplink fast convergence feature is applicable to bridges that are acting as access switches to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on RoamAbout switches that are in the network core.

Example

The following command enables uplink fast convergence:

```
RBT-8100# set spantree uplinkfast enable
success: change accepted.
```

Related Commands

show spantree uplinkfast on page 12-33

show spantree

Displays STP configuration and port-state information.

Syntax

show spantree [**port** *port-list* | **vlan** *vlan-id*] [**active**]

Parameters

port *port-list*	List of ports. If you do not specify any ports, MSS displays STP information for all ports.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays STP information for all VLANs.
active	Displays information for only the active (forwarding) ports.

Defaults

None.

Mode

All.

Example

The following command displays STP information for VLAN *default*:

```
RBT-8100# show spantree vlan default
VLAN     1
Spanning Tree Mode           PVST+
Spanning Tree Type           IEEE
Spanning Tree Enabled

Designated Root              00-02-4a-70-49-f7
Designated Root Priority     32768
Designated Root Path Cost    19
Designated Root Port         1
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-02-76-f7
Bridge ID Priority           32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port               Vlan      STP-State     Cost   Prio    Portfast
-------------------------------------------------------------------------------
1                   1        Forwarding      19   128     Disabled
2                   1        STP Off         19   128     Disabled
3                   1        Disabled        19   128     Disabled
4                   1        Disabled        19   128     Disabled
5                   1        Disabled        19   128     Disabled
6                   1        Disabled        19   128     Disabled
7                   1        Disabled        19   128     Disabled
```

```
8                   1        Disabled        19   128     Disabled
10                  1        Forwarding      19   128     Disabled
15                  1        Disabled        19   128     Disabled
16                  1        Disabled        19   128     Disabled
17                  1        STP Off         19   128     Disabled
18                  1        STP Off         19   128     Disabled
19                  1        Disabled        19   128     Disabled
20                  1        Disabled        19   128     Disabled
21                  1        Disabled         4   128     Disabled
22                  1        Disabled         4   128     Disabled
```

Table 12-2 describes the fields in this display.

Table 12-2 Output for show spantree

Output	What It Displays...
VLAN	VLAN number.
Spanning Tree Mode	In the current software version, the mode is always *PVST+*, which means Per VLAN Spanning Tree+.
Spanning Tree Type	In the current software version, the type is always *IEEE*, which means STP is based on the IEEE 802 standards.
Spanning Tree Enabled	State of STP on the VLAN.
Designated Root	MAC address of the spanning tree's root bridge.
Designated Root Priority	Bridge priority of the root bridge.
Designated Root Path Cost	Cumulative cost from this bridge to the root bridge. If this RoamAbout switch is the root bridge, then the root cost is 0.
Designated Root Port	Port through which this RoamAbout switch reaches the root bridge. If this RoamAbout switch is the root bridge, this field says *We are the root*.
Root Max Age	Maximum acceptable age for hello packets on the root bridge.
Root Hello Time	Hello interval on the root bridge.
Root Forward Delay	Forwarding delay value on the root bridge.
Bridge ID MAC ADDR	This RoamAbout switch's MAC address.
Bridge ID Priority	This RoamAbout switch's bridge priority.
Bridge Max Age	This RoamAbout switch's maximum acceptable age for hello packets.
Bridge Hello Time	This RoamAbout switch's hello interval.
Bridge Forward Delay	This RoamAbout switch's forwarding delay value.
Port	Port number. **Note:** Only network ports are listed. STP does not apply to Access Point ports or wired authentication ports.
Vlan	VLAN ID.

Table 12-2 Output for show spantree (continued)

Output	What It Displays...
STP-State or Port-State	STP state of the port: • Blocking—The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. • Disabled—This state can indicate any of the following conditions: - The port is inactive. - The port is disabled. - STP is enabled on the port but the port is not forwarding traffic. (The port is active and enabled but STP has just started to come up.) • Forwarding—The port is forwarding Layer 2 traffic. • Learning—The port is learning the locations of other devices in the spanning tree before changing state to forwarding. • Listening—The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding. • STP Off—STP is disabled on the port.
Cost	STP cost of the port.
Prio	STP priority of the port.
Portfast	State of the uplink fast convergence feature: • Enabled • Disabled

Related Commands

show spantree blockedports on page 12-24

show spantree backbonefast

Indicates whether the STP backbone fast convergence feature is enabled or disabled.

Syntax

show spantree backbonefast

Parameters

None.

Defaults

None.

Mode

All.

Example

The following example shows the command output on a RoamAbout switch with backbone fast convergence enabled:

```
RBT-8100# show spantree backbonefast
 Backbonefast is enabled
```

Related Commands

set spantree backbonefast on page 12-8

show spantree blockedports

Lists information about RoamAbout switch ports that STP has blocked on one or all of its VLANs.

Syntax

show spantree blockedports [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays information for blocked ports on all VLANs.

Defaults

None.

Mode

All.

Usage

The command lists information separately for each VLAN.

Example

The following command shows information about blocked ports on a RoamAbout switch for the *default* VLAN (VLAN 1):

```
RBT-8100# show spantree blockedports vlan default

Port               Vlan       Port-State    Cost   Prio   Portfast
-------------------------------------------------------------------------
22                  190        Blocking         4   128     Disabled

Number of blocked ports (segments) in VLAN 1 : 1
```

The port information is the same as the information displayed by the **show spantree** command. See Table 12-2 on page 12-21.

Related Commands

show spantree on page 12-20

show spantree portfast

Displays STP uplink fast convergence information for all network ports or for one or more network ports.

Syntax

show spantree portfast [*port-list*]

Parameters

port-list	List of ports. If you do not specify any ports, MSS displays uplink fast convergence information for all ports.

Defaults

None.

Mode

All.

Example

The following command shows uplink fast convergence information for all ports:

```
RBT-8100# show spantree portfast
Port                        Vlan   Portfast
--------------------------- ----   ----------
1                           1      disable
2                           1      disable
3                           1      disable
4                           1      enable
5                           1      disable
6                           1      disable
7                           1      disable
8                           1      disable
10                          1      disable
15                          1      disable
16                          1      disable
17                          1      disable
18                          1      disable
19                          1      disable
20                          1      disable
21                          1      disable
22                          1      disable
11                          2      enable
12                          2      disable
13                          2      disable
14                          2      enable
```

Table 12-3 describes the fields in this display.

Table 12-3 Output for show spantree portfast

Output	What It Displays...
Port	Port number.
VLAN	VLAN number.
Portfast	State of the uplink fast convergence feature: • Enable • Disable

Related Commands

set spantree portfast on page 12-14

show spantree portvlancost

Displays the cost of a port on a path to the STP root bridge, for each of the port's VLANs.

Syntax

show spantree portvlancost *port-list*

Parameters

port-list	List of ports.

Defaults

None.

Mode

All.

Example

The following command shows the STP port cost of port 1:

```
RBT-8100# show spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

Related Commands

- clear spantree portcost on page 12-2
- clear spantree portvlancost on page 12-4
- set spantree portcost on page 12-12
- set spantree portvlancost on page 12-16
- show spantree on page 12-20

show spantree statistics

Displays STP statistics for one or more RoamAbout switch network ports.

Syntax

show spantree statistics [*port-list* [**vlan** *vlan-id*]]

Parameters

port-list	List of ports. If you do not specify any ports, MSS displays STP statistics for all ports.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

Defaults

None.

Mode

All.

Usage

The command displays statistics separately for each port.

Example

The following command shows STP statistics for port 1:

```
RBT-8100# show spantree statistics 1

BPDU related parameters


Port 1                    VLAN 1
spanning tree enabled for VLAN = 1
port spanning tree                          enabled
state                                       Forwarding
port_id                                     0x8015
port_number                                 0x15
path cost                                   0x4
message age (port/VLAN)                     0(20)
designated_root                             00-0b-0e-00-04-30
designated cost                             0x0
designated_bridge                           00-0b-0e-00-04-30
designated_port                             38
top_change_ack                              FALSE
config_pending                              FALSE
port_inconsistency                          none
```

```
            Port based information statistics

config BPDU's xmitted(port/VLAN)         0 (1)
config BPDU's received(port/VLAN)        21825 (43649)
tcn BPDU's xmitted(port/VLAN)            0 (0)
tcn BPDU's received(port/VLAN)           2 (2)
forward transition count (port/VLAN)     1 (1)
scp failure count                        0
root inc trans count (port/VLAN)         1 (1)
inhibit loopguard                        FALSE
loop inc trans count                     0 (0)

            Status of Port Timers

forward delay timer                      INACTIVE
forward delay timer value                15
message age timer                        ACTIVE
message age timer value                  0
topology change timer                    INACTIVE
topology change timer value              0
hold timer                               INACTIVE
hold timer value                         0
delay root port timer                    INACTIVE
delay root port timer value              0
delay root port timer restarted is       FALSE


            VLAN based information & statistics

spanning tree type                       ieee
spanning tree multicast address          01-00-0c-cc-cc-cd
bridge priority                          32768
bridge MAC address                       00-0b-0e-12-34-56
bridge hello time                        2
bridge forward delay                     15
topology change initiator:               0
last topology change occured:            Tue Jul 01 2003 22:33:36.
topology change                          FALSE
topology change time                     35
topology change detected                 FALSE
topology change count                    1
topology change last recvd. from         00-0b-0e-02-76-f6

            Other port specific info

dynamic max age transition               0
port BPDU ok count                       21825
msg age expiry count                     0
link loading                             0
```

```
BPDU in processing                          FALSE
num of similar BPDU's to process            0
received_inferior_bpdu                      FALSE
next state                                  0
src MAC count                               21807
total src MAC count                         21825
curr_src_mac                                00-0b-0e-00-04-30
next_src_mac                                00-0b-0e-02-76-f6
```

Table 12-4 describes the fields in this display.

Table 12-4 Output for show spantree statistics

Output	What It Displays...
Port	Port number.
VLAN	VLAN ID.
Spanning Tree enabled for vlan	State of the STP feature on the VLAN.
port spanning tree	State of the STP feature on the port.
state	STP state of the port: • Blocking—The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. • Disabled—The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected. • Forwarding—The port is forwarding Layer 2 traffic. • Learning—The port is learning the locations of other devices in the spanning tree before changing state to forwarding. • Listening—The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.
port_id	STP port ID.
port_number	STP port number.
path cost	Cost to use this port to reach the root bridge. This is part of the total path cost (designated cost).
message age	Age of the protocol information for a port and the value of the maximum age parameter (shown in parenthesis) recorded by the switch.
designated_root	MAC address of the root bridge.
designated cost	Total path cost to reach the root bridge.
designated_bridge	Bridge to which this switch forwards traffic away from the root bridge.
designated_port	STP port through which this switch forwards traffic away from the root bridge.
top_change_ack	Value of the topology change acknowledgment flag in the next configured bridge protocol data unit (BPDU) to be transmitted on the associated port. The flag is set in reply to a topology change notification BPDU.

Table 12-4 Output for show spantree statistics (continued)

Output	What It Displays...
config_pending	Indicates whether a configured BPDU is to be transmitted on expiration of the hold timer for the port.
port_inconsistency	Indicates whether the port is in an inconsistent state.
config BPDU's xmitted	Number of BPDUs transmitted from the port. A number in parentheses indicates the number of configured BPDUs transmitted by the RoamAbout switch for this VLAN's spanning tree.
config BPDU's received	Number of BPDUs received by this port. A number in parentheses indicates the number of configured BPDUs received by the RoamAbout switch for this VLAN's spanning tree.
tcn BPDU's xmitted	Number of topology change notification (TCN) BDPUs transmitted on this port.
tcn BPDU's received	Number of TCN BPDUs received on this port.
forward transition count	Number of times the port state transitioned to the forwarding state.
scp failure count	Number of service control point (SCP) failures.
root inc trans count	Number of times the root bridge changed.
inhibit loopguard	State of the loop guard. In the current release, the state is always FALSE.
loop inc trans count	Number of loops that have occurred.
forward delay timer	Status of the forwarding delay timer. This timer monitors the time spent by a port in the listening and learning states.
forward delay timer value	Current value of the forwarding delay timer, in seconds.
message age timer	Status of the message age timer. This timer measures the age of the received protocol information recorded for a port.
message age timer value	Current value of the message age timer, in seconds.
topology change timer	Status of the topology change timer. This timer determines the time period during which configured BPDUs are transmitted with the topology change flag set by this RoamAbout switch when it is the root bridge, after detection of a topology change.
topology change timer value	Current value of the topology change timer, in seconds.
hold timer	Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port.
hold timer value	Current value of the hold timer, in seconds.
delay root port timer	Status of the delay root port timer, which enables fast convergence when uplink fast convergence is enabled.
delay root port timer value	Current value of the delay root port timer.
delay root port timer restarted is	Whether the delay root port timer has been restarted.
spanning tree type	Type of spanning tree. The type is always IEEE.
spanning tree multicast address	Destination address used to send out configured BPDUs on a bridge port.

Table 12-4 Output for show spantree statistics (continued)

Output	What It Displays...
bridge priority	STP priority of this RoamAbout switch.
bridge MAC address	MAC address of this RoamAbout switch.
bridge hello time	Value of the hello timer interval, in seconds, when this RoamAbout switch is the root or is attempting to become the root.
bridge forward delay	Value of the forwarding delay interval, in seconds, when this RoamAbout switch is the root or is attempting to become the root.
topology change initiator	Port number that initiated the most recent topology change.
last topology change occurred	System time when the most recent topology change occurred.
topology change	Value of the topology change flag in configuration BPDUs to be transmitted by this RoamAbout switch on VLANs for which the switch is the designated bridge.
topology change time	Time period, in seconds, during which BPDUs are transmitted with the topology change flag set by this RoamAbout switch when it is the root bridge, after detection of a topology change. It is equal to the sum of the switch's maximum age and forwarding delay parameters.
topology change detected	Indicates whether a topology change has been detected by the switch.
topology change count	Number of times the topology change has occurred.
topology change last recvd. from	MAC address of the bridge from which the RoamAbout switch last received a topology change.
dynamic max age transition	Number of times the maximum age parameter was changed dynamically.
port BPDU ok count	Number of valid port BPDUs received.
msg age expiry count	Number of expired messages.
link loading	Indicates whether the link is oversubscribed.
BPDU in processing	Indicates whether BPDUs are currently being processed.
num of similar BPDU's to process	Number of similar BPDUs received on a port that need to be processed.
received_inferior_bpdu	Indicates whether the port has received an inferior BPDU or a response to a Root Link Query (RLQ) BPDU.
next state	Port state before it is set by STP.
src MAC count	Number of BPDUs with the same source MAC address.
total src MAC count	Number of BPDUs with all the source MAC addresses.
curr_src_mac	Source MAC address of the current received BPDU.
next_src_mac	Other source MAC address from a different source.

Related Commands

clear spantree statistics on page 12-6

show spantree uplinkfast

Displays uplink fast convergence information for one VLAN or all VLANs.

Syntax

show spantree uplinkfast [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

Defaults

None.

Mode

All.

Example

The following command shows uplink fast convergence information for all VLANs:

```
RBT-8100# show spantree uplinkfast
 VLAN    port    list
-------------------------------------------------------------------------------
1       1(fwd),2,3
```

Table 12-5 describes the fields in this display.

Table 12-5 Output for show spantree uplinkfast

Output	What It Displays...
VLAN	VLAN number.
port list	Ports in the uplink group. The port that is forwarding traffic is indicated by *fwd*. The other ports are blocking traffic.

Related Commands

set spantree uplinkfast on page 12-19.

13

IGMP Snooping Commands

Use Internet Group Management Protocol (IGMP) snooping commands to configure and manage multicast traffic reduction on a RoamAbout switch. This chapter presents IGMP snooping commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear igmp statistics	13-2
set igmp	13-3
set igmp lmqi	13-4
set igmp mrouter	13-5
set igmp mrsol	13-6
set igmp mrsol mrsi	13-7
set igmp oqi	13-8
set igmp proxy-report	13-9
set igmp qi	13-10
set igmp qri	13-11
set igmp querier	13-12
set igmp receiver	13-13
set igmp rv	13-14
show igmp	13-15
show igmp mrouter	13-19
show igmp querier	13-21
show igmp receiver-table	13-23
show igmp statistics	13-25

clear igmp statistics

Clears IGMP statistics counters on one VLAN or all VLANs on a RoamAbout switch and resets them to 0.

Syntax

clear igmp statistics [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, IGMP statistics are cleared for all VLANs.

Defaults

None.

Mode

Enabled.

Example

The following command clears IGMP statistics for all VLANs:

```
RBT-8100# clear igmp statistics
IGMP statistics cleared for all vlans
```

Related Commands

show igmp statistics on page 13-25

set igmp

Disables or reenables IGMP snooping on one VLAN or all VLANs on a RoamAbout switch.

Syntax

set igmp {**enable** | **disable**} [**vlan** *vlan-id*]

Parameters

enable	Enables IGMP snooping.
disable	Disables IGMP snooping.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, IGMP snooping is disabled or reenabled on all VLANs.

Defaults

IGMP snooping is enabled on all VLANs by default.

Mode

Enabled.

Example

The following command disables IGMP snooping on VLAN *orange*:

```
RBT-8100# set igmp disable vlan orange
success: change accepted.
```

Related Commands

show igmp on page 13-15

set igmp lmqi

Changes the IGMP last member query interval timer on one VLAN or all VLANs on a RoamAbout switch.

Syntax

set igmp lmqi *tenth-seconds* [**vlan** *vlan-id*]

Parameters

lmqi *tenth-seconds*	Amount of time (in tenths of a second) that the RoamAbout switch waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the switch also sends a leave message for the group to multicast routers. You can specify a value from 1 through 65,535.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults

The default last member query interval is 10 tenths of a second (1 second).

Mode

Enabled.

Example

The following command changes the last member query interval on VLAN *orange* to 5 tenths of a second:

```
RBT-8100# set igmp lmqi 5 vlan orange
success: change accepted.
```

Related Commands

- set igmp oqi on page 13-8
- set igmp qi on page 13-10
- set igmp mrouter on page 13-5

set igmp mrouter

Adds or removes a port in a RoamAbout switch's list of ports on which it forwards traffic to multicast routers. Static multicast ports are immediately added to or removed from the list of router ports and do not age out.

Syntax

set igmp mrouter port *port-list* {**enable** | **disable**}

Parameters

port *port-list*	Port list. MSS adds or removes the specified ports in the list of static multicast router ports.
enable	Adds the port to the list of static multicast router ports.
disable	Removes the port from the list of static multicast router ports.

Defaults

By default, no ports are static multicast router ports.

Mode

Enabled.

Usage

You cannot add AP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples

The following command adds port 9 as a static multicast router port:

```
RBT-8100# set igmp mrouter port 9 enable
success: change accepted.
```

The following command removes port 9 from the static multicast router port list:

```
RBT-8100# set igmp mrouter port 9 disable
success: change accepted.
```

Related Commands

show igmp mrouter on page 13-19

set igmp mrsol

Enables or disables multicast router solicitation by a RoamAbout switch on one VLAN or all VLANs.

Syntax

set igmp mrsol {**enable** | **disable**} [**vlan** *vlan-id*]

Parameters

enable	Enables multicast router solicitation.
disable	Disables multicast router solicitation.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, multicast router solicitation is disabled or enabled on all VLANs.

Defaults

Multicast router solicitation is disabled on all VLANs by default.

Mode

Enabled.

Example

The following command enables multicast router solicitation on VLAN *orange*:

```
RBT-8100# set igmp mrsol enable vlan orange
success: change accepted.
```

Related Commands

set igmp mrsol mrsi on page 13-7

set igmp mrsol mrsi

Changes the interval between multicast router solicitations by a RoamAbout switch on one VLAN or all VLANs.

Syntax

set igmp mrsol mrsi *seconds* [**vlan** *vlan-id*]

Parameters

seconds	Number of seconds between multicast router solicitations. You can specify a value from 1 through 65,535.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS changes the multicast router solicitation interval for all VLANs.

Defaults

The interval between multicast router solicitations is 30 seconds by default.

Mode

Enabled.

Example

The following example changes the multicast router solicitation interval to 60 seconds:

```
RBT-8100# set igmp mrsol mrsi 60
success: change accepted.
```

Related Commands

set igmp mrsol on page 13-6

set igmp oqi

Changes the IGMP other-querier-present interval timer on one VLAN or all VLANs on a RoamAbout switch.

Syntax

set igmp oqi *seconds* [**vlan** *vlan-id*]

Parameters

oqi *seconds*	Number of seconds that the RoamAbout switch waits for a general query to arrive before electing itself the querier. You can specify a value from 1 through 65,535.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults

The default other-querier-present interval is 255 seconds (4.25 minutes).

Mode

Enabled.

Usage

A RoamAbout switch cannot become the querier unless the pseudo-querier feature is enabled on the switch. When the feature is enabled, the switch becomes the querier for a subnet so long as the switch does not receive a query message from a router with a lower IP address than the IP address of the switch in that subnet. To enable the pseudo-querier feature, use **set igmp querier**.

Example

The following command changes the other-querier-present interval on VLAN *orange* to 200 seconds:

```
RBT-8100# set igmp oqi 200 vlan orange
success: change accepted.
```

Related Commands

- set igmp lmqi on page 13-4
- set igmp qi on page 13-10
- set igmp qri on page 13-11
- set igmp querier on page 13-12
- set igmp mrouter on page 13-5
- set igmp rv on page 13-14

set igmp proxy-report

Disables or reenables proxy reporting by a RoamAbout switch on one VLAN or all VLANs.

Syntax

set igmp proxy-report {**enable** | **disable**} [**vlan** *vlan-id*]

Parameters

enable	Enables proxy reporting.
disable	Disables proxy reporting.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, proxy reporting is disabled or reenabled on all VLANs.

Defaults

Proxy reporting is enabled on all VLANs by default.

Mode

Enabled.

Usage

Proxy reporting reduces multicast overhead by sending only one membership report for a group to the multicast routers and discarding other membership reports for the same group. If you disable proxy reporting, the RoamAbout switch sends all membership reports to the routers, including multiple reports for the same group.

Example

The following example disables proxy reporting on VLAN *orange*:

```
RBT-8100# set igmp proxy-report disable vlan orange
success: change accepted.
```

Related Commands

show igmp on page 13-15

set igmp qi

Changes the IGMP query interval timer on one VLAN or all VLANs on a RoamAbout switch.

Syntax

```
set igmp qi seconds [vlan vlan-id]
```

Parameters

qi *seconds*	Number of seconds that elapse between general queries sent by the RoamAbout switch when the switch is the querier for the subnet. You can specify a value from 1 through 65,535.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults

The default query interval is 125 seconds.

Mode

Enabled.

Usage

The query interval is applicable only when the RoamAbout switch is querier for the subnet. For the switch to become the querier, the pseudo-querier feature must be enabled on the switch and the switch must have the lowest IP address among all the devices eligible to become a querier. To enable the pseudo-querier feature, use the **set igmp querier** command.

Example

The following command changes the query interval on VLAN *orange* to 100 seconds:

```
RBT-8100# set igmp qi 100 vlan orange
success: change accepted.
```

Related Commands

- set igmp lmqi on page 13-4
- set igmp oqi on page 13-8
- set igmp qri on page 13-11
- set igmp querier on page 13-12
- set igmp mrouter on page 13-5
- set igmp rv on page 13-14

set igmp qri

Changes the IGMP query response interval timer on one VLAN or all VLANs on a RoamAbout switch.

Syntax

set igmp qri *tenth-seconds* [**vlan** *vlan-id*]

Parameters

qri *tenth-seconds*	Amount of time (in tenths of a second) that the RoamAbout switch waits for a receiver to respond to a group-specific query message before removing the receiver from the receiver list for the group. You can specify a value from 1 through 65,535.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults

The default query response interval is 100 tenths of a second (10 seconds).

Mode

Enabled.

Usage

The query response interval is applicable only when the RoamAbout switch is querier for the subnet. For the switch to become the querier, the pseudo-querier feature must be enabled on the switch and the switch must have the lowest IP address among all the devices eligible to become a querier. To enable the pseudo-querier feature, use **set igmp querier**.

Example

The following command changes the query response interval on VLAN *orange* to 50 tenths of a second (5 seconds):

```
RBT-8100# set igmp qri 50 vlan orange
success: change accepted.
```

Related Commands

- set igmp lmqi on page 13-4
- set igmp oqi on page 13-8
- set igmp qi on page 13-10
- set igmp querier on page 13-12
- set igmp rv on page 13-14

set igmp querier

Enables or disables the IGMP pseudo-querier on a RoamAbout switch, on one VLAN or all VLANs.

Syntax

set igmp querier {**enable** | **disable**} [**vlan** *vlan-id*]

Parameters

enable	Enables the pseudo-querier.
disable	Disables the pseudo-querier.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, the pseudo-querier is enabled or disabled on all VLANs.

Defaults

The pseudo-querier is disabled on all VLANs by default.

Mode

Enabled.

Usage

recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

Example

The following example enables the pseudo-querier on the *orange* VLAN:

```
RBT-8100# set igmp querier enable vlan orange
success: change accepted.
```

Related Commands

show igmp querier on page 13-21

set igmp receiver

Adds or removes a network port in the list of ports on which a RoamAbout switch forwards traffic to multicast receivers. Static multicast receiver ports are immediately added to or removed from the list of receiver ports and do not age out.

Syntax

set igmp receiver port *port-list* {**enable** | **disable**}

Parameters

port *port-list*	Network port list. MSS adds the specified ports to the list of static multicast receiver ports.
enable	Adds the port to the list of static multicast receiver ports.
disable	Removes the port from the list of static multicast receiver ports.

Defaults

By default, no ports are static multicast receiver ports.

Mode

Enabled.

Usage

You cannot add AP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Example

The following command adds port 7 as a static multicast receiver port:

```
RBT-8100# set igmp receiver port 7 enable
success: change accepted.
```

The following command removes port 7 from the list of static multicast receiver ports:

```
RBT-8100# set igmp receiver port 7 disable
success: change accepted.
```

Related Commands

show igmp receiver-table on page 13-23

set igmp rv

Changes the robustness value for one VLAN or all VLANs on a RoamAbout switch. Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network.

Syntax

set igmp rv *num* [**vlan** *vlan-id*]

Parameters

num	Robustness value. You can specify a value from 2 through 255. Set the robustness value higher to adjust for more traffic loss.
vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS changes the robustness value for all VLANs.

Defaults

The default robustness value for all VLANs is 2.

Mode

Enabled.

Example

The following example changes the robustness value on VLAN *orange* to 4:

```
RBT-8100# set igmp rv 4 vlan orange
success: change accepted.
```

Related Commands

- set igmp oqi on page 13-8
- set igmp qi on page 13-10
- set igmp qri on page 13-11

show igmp

Displays IGMP configuration information and statistics for one VLAN or all VLANs.

Syntax

show igmp [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays IGMP information for all VLANs.

Defaults

None.

Mode

All.

Example

The following command displays IGMP information for VLAN *orange*:

```
RBT-8100# show igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2 Multicast
router information:
Port Mrouter-IPaddr Mrouter-MAC        Type  TTL
---- --------------- ----------------- ----- -----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp    17
Group           Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
      224.0.0.2 none            none              none undef
237.255.255.255    5     10.10.10.11 00:02:04:06:08:0b   258
237.255.255.255    5     10.10.10.13 00:02:04:06:08:0d   258
237.255.255.255    5     10.10.10.14 00:02:04:06:08:0e   258
237.255.255.255    5     10.10.10.12 00:02:04:06:08:0c   258
237.255.255.255    5     10.10.10.10 00:02:04:06:08:0a   258
Querier information:
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
IGMP vlan member ports: 10, 12, 11, 14, 16, 15, 13, 18, 17, 1, 20, 21, 2,
22, 19, 4, 6, 5, 3, 8, 7, 9
IGMP static ports: none
IGMP statistics for vlan orange:
```

```
IGMP message type Received Transmitted Dropped
----------------- -------- ----------- -------
General-Queries          0           0       0
GS-Queries               0           0       0
Report V1                0           0       0
Report V2                5           1       4
Leave                    0           0       0
Mrouter-Adv              0           0       0
Mrouter-Term             0           0       0
Mrouter-Sol             50         101       0
DVMRP                    4           4       0
PIM V1                   0           0       0
PIM V2                   0           0       0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

Table 13-1 describes the fields in this display.

Table 13-1 Output for show igmp

Output	What It Displays...
VLAN	VLAN name. MSS displays information separately for each VLAN.
IGMP is enabled (disabled)	IGMP state.
Proxy reporting	Proxy reporting state.
Mrouter solicitation	Multicast router solicitation state.
Querier functionality	Pseudo-querier state.
Configuration values (qi)	Query interval.
Configuration values (oqi)	Other-querier-present interval.
Configuration values (qri)	Query response interval.
Configuration values (lmqi)	Last member query interval.
Configuration values (rvalue)	Robustness value.
Multicast router information	List of multicast routers and active multicast groups. The fields containing this information are described separately. The **show igmp mrouter** command shows the same information.
Port	Number of the physical port through which the RoamAbout switch can reach the router.
Mrouter-IPaddr	IP address of the multicast router interface.
Mrouter-MAC	MAC address of the multicast router interface.

Table 13-1 Output for show igmp (continued)

Output	What It Displays...
Type	How the RoamAbout switch learned that the port is a multicast router port: • conf — Static multicast port configured by an administrator • madv—Multicast advertisement • quer—IGMP query • dvmrp—Distance Vector Multicast Routing Protocol (DVMRP) • pimv1—Protocol Independent Multicast (PIM) version 1 • pimv2—PIM version 2
TTL	Number of seconds before this entry ages out if not refreshed. For static multicast router entries, the time-to-live (TTL) value is *undef*. Static multicast router entries do not age out.
Group	IP address of a multicast group. The **show igmp receiver-table** command shows the same information as these receiver fields.
Port	Physical port through which the RoamAbout switch can reach the group's receiver.
Receiver-IP	IP address of the client receiving the group.
Receiver-MAC	MAC address of the client receiving the group.
TTL	Number of seconds before this entry ages out if the RoamAbout switch does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is *undef*. Static multicast receiver entries do not age out.
Querier information	Information about the subnet's multicast querier. If the querier is another device, the fields described below are applicable. If the querier is the RoamAbout switch itself, the output indicates how many seconds remain until the next general query message. If IGMP snooping does not detect a querier, the output indicates this. The **show igmp querier** command shows the same information.
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier.
Querier-MAC	MAC address of the querier.
TTL	Number of seconds before this entry ages out if the RoamAbout switch does not receive a query message from the querier.
IGMP vlan member ports	Physical ports in the VLAN. This list includes all network ports configured to be in the VLAN and all ports MSS dynamically assigns to the VLAN when a user assigned to the VLAN becomes a receiver. For example, the list can include an AP access port that is not configured to be in the VLAN when a user associated with the Access Point on that port becomes a receiver for a group. When all receivers on a dynamically added port age out, MSS removes the port from the list.
IGMP static ports	Static receiver ports.
IGMP statistics	Multicast message and packet statistics. These are the same statistics displayed by the **show igmp statistics** command.

Related Commands

- show igmp mrouter on page 13-19
- show igmp querier on page 13-21
- show igmp receiver-table on page 13-23
- show igmp statistics on page 13-25

show igmp mrouter

Displays the multicast routers in a RoamAbout switch's subnet, on one VLAN or all VLANs. Routers are listed separately for each VLAN, according to the port number through which the switch can reach the router.

Syntax

show igmp mrouter [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays the multicast routers in all VLANs.

Defaults

None.

Mode

All.

Example

The following command displays the multicast routers in VLAN *orange*:

```
RBT-8100# show igmp mrouter vlan orange
Multicast routers for vlan orange
Port Mrouter-IPaddr  Mrouter-MAC       Type  TTL
---- --------------- ----------------- ----- -----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp    33
```

Table 13-2 describes the fields in this display.

Table 13-2 Output for show igmp mrouter

Output	What It Displays...
Multicast routers for vlan	VLAN containing the multicast routers. Ports are listed separately for each VLAN.
Port	Number of the physical port through which the RoamAbout switch can reach the router.
Mrouter-IPaddr	IP address of the multicast router.
Mrouter-MAC	MAC address of the multicast router.
Type	How the RoamAbout switch learned that the port is a multicast router port: • conf — Static multicast port configured by an administrator • madv—Multicast advertisement • quer—IGMP query • dvmrp—Distance Vector Multicast Routing Protocol (DVMRP) • pimv1—Protocol Independent Multicast (PIM) version 1 • pimv2—PIM version 2

Table 13-2 Output for show igmp mrouter (continued)

Output	What It Displays...
TTL	Number of seconds before this entry ages out if unused. For static multicast router entries, the TTL value is *undef*. Static multicast router entries do not age out.

Related Commands

- set igmp mrouter on page 13-5
- show igmp mrouter on page 13-19

show igmp querier

Displays information about the active multicast querier, on one VLAN or all VLANs. Queriers are listed separately for each VLAN. Each VLAN can have only one querier.

Syntax

show igmp querier [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays querier information for all VLANs.

Defaults

None.

Mode

Enabled.

Examples

The following command displays querier information for VLAN *orange*:

```
RBT-8100# show igmp querier vlan orange
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
```

The following command shows the information MSS displays when the querier is the RoamAbout switch itself:

```
RBT-8100# show igmp querier vlan default
Querier for vlan default:
I am the querier for vlan default, time to next query is 20
```

The output indicates how many seconds remain before the pseudo-querier on the switch broadcasts the next general query report to IP address 224.0.0.1, the multicast all-systems group.

If IGMP snooping does not detect a querier, the output indicates this finding, as shown in the following example:

```
RBT-8100# show igmp querier vlan red
Querier for vlan red:
There is no querier present on vlan red
```

This condition does not necessarily indicate a problem. For example, election of the querier might be in progress.

Table 13-3 on page 13-22 describes the fields in the display when a querier other than the RoamAbout switch is present.

Table 13-3 Output for show igmp querier

Output	What It Displays...
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier interface.
Querier-MAC	MAC address of the querier interface.
TTL	Number of seconds before this entry ages out if the RoamAbout switch does not receive a query message from the querier.

Related Commands

set igmp querier on page 13-12

show igmp receiver-table

Displays the receivers to which a RoamAbout switch forwards multicast traffic. You can display receivers for all VLANs, a single VLAN, or a group or groups identified by group address and network mask.

Syntax

show igmp receiver-table [**vlan** *vlan-id*] [**group** *group-ip-addr/mask-length*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays the multicast receivers on all VLANs.
group *group-ip-addr/mask-length*	IP address and subnet mask of a multicast group, in CIDR format (for example, 239.20.20.10/24). If you do not specify a group address, MSS displays the multicast receivers for all groups.

Defaults

None.

Mode

All.

Examples

The following command displays all multicast receivers in VLAN *orange*:

```
RBT-8100# show igmp receiver-table vlan orange
VLAN: orange
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
      224.0.0.2 none            none              none undef
237.255.255.255    5     10.10.10.11 00:02:04:06:08:0b   179
237.255.255.255    5     10.10.10.13 00:02:04:06:08:0d   179
237.255.255.255    5     10.10.10.14 00:02:04:06:08:0e   179
237.255.255.255    5     10.10.10.12 00:02:04:06:08:0c   179
237.255.255.255    5     10.10.10.10 00:02:04:06:08:0a   179
```

The following command lists all receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs:

```
RBT-8100# show igmp receiver-table group 237.255.255.0/24
VLAN: red
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
237.255.255.2      2     10.10.20.19 00:02:04:06:09:0d   112
237.255.255.119    3     10.10.30.31 00:02:04:06:01:0b   112

VLAN: green
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
```

```
237.255.255.17    11     10.10.40.41 00:02:06:08:02:0c    12
237.255.255.255    6     10.10.60.61 00:05:09:0c:0a:01   111
```

Table 13-4 describes the fields in this display.

Table 13-4 Output for show igmp receiver-table

Output	What It Displays...
VLAN	VLAN that contains the multicast receiver ports. Ports are listed separately for each VLAN.
Session	IP address of the multicast group being received.
Port	Physical port through which the RoamAbout switch can reach the receiver.
Receiver-IP	IP address of the receiver.
Receiver-MAC	MAC address of the receiver.
TTL	Number of seconds before this entry ages out if the RoamAbout switch does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is *undef*. Static multicast receiver entries do not age out.

Related Commands

set igmp receiver on page 13-13

show igmp statistics

Displays IGMP statistics.

Syntax

show igmp statistics [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	VLAN name or number. If you do not specify a VLAN, MSS displays IGMP statistics for all VLANs.

Defaults

None.

Mode

All.

Example

The following command displays IGMP statistics for VLAN *orange*:

```
RBT-8100# show igmp statistics vlan orange
IGMP statistics for vlan orange:

IGMP message type Received Transmitted Dropped
----------------- -------- ----------- -------
General-Queries          0           0       0
GS-Queries               0           0       0
Report V1                0           0       0
Report V2                5           1       4
Leave                    0           0       0
Mrouter-Adv              0           0       0
Mrouter-Term             0           0       0
Mrouter-Sol             50         101       0
DVMRP                    4           4       0
PIM V1                   0           0       0
PIM V2                   0           0       0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

Table 13-5 describes the fields in this display.

Table 13-5 Output for show igmp statistics

Output	What It Displays...
IGMP statistics for vlan	VLAN name. Statistics are listed separately for each VLAN.
IGMP message type	Type of IGMP message: • General-Queries—General group membership queries sent by the multicast querier (multicast router or pseudo-querier). • GS-Queries—Group-specific queries sent by the the multicast querier to determine whether there are receivers for a specific group. • Report V1—IGMP version 1 group membership reports sent by clients who want to be receivers for the groups. • Report V2—IGMP version 2 group membership reports sent by clients who want to be receivers for the groups. • Leave—IGMP version 2 leave messages sent by clients who want to stop receiving traffic for a group. Leave messages apply only to IGMP version 2. • Mrouter-Adv—Multicast router advertisement packets. A multicast router sends this type of packet to advertise the IP address of the sending interface as a multicast router interface.
IGMP message type	Type of IGMP message, continued: • Mrouter-Term—Multicast router termination messages. A multicast router sends this type of message when multicast forwarding is disabled on the router interface, the router interface is administratively disabled, or the router itself is gracefully shutdown. • Mrouter-Sol—Multicast router solicitation messages. A multicast client or a RoamAbout switch sends this type of message to immediately solicit multicast router advertisement messages from the multicast routers in the subnet. • DVMRP—Distance Vector Multicast Routing Protocol (DVMRP) messages. Multicast routers running DVMRP exchange multicast information with these messages. • PIM V1—Protocol Independent Multicast (PIM) version 1 messages. Multicast routers running PIMv1 exchange multicast information with these messages. • PIM V2—PIM version 2 messages.
Received	Number of packets received.
Transmitted	Number of packets transmitted. This number includes both multicast packets originated by the RoamAbout switch and multicast packets received and then forwarded by the switch.
Dropped	Number of IGMP packets dropped by the RoamAbout switch.
Topology notifications	Number of Layer 2 topology change notifications received by the RoamAbout switch. **Note:** In the current software version, the value in this field is always 0.
Packets with unknown IGMP type	Number of multicast packets received with an unrecognized multicast type.
Packets with bad length	Number of packets with an invalid length.

Table 13-5 Output for show igmp statistics (continued)

Output	What It Displays...
Packets with bad IGMP checksum	Number of packets with an invalid IGMP checksum value.
Packets dropped	Number of multicast packets dropped by the RoamAbout switch.

Related Commands

clear igmp statistics on page 13-2

14

Security ACL Commands

Use security ACL commands to configure and monitor security access control lists (ACLs). Security ACLs filter packets to restrict or permit network usage by certain users or traffic types, and can assign to packets a class of service (CoS) to define the priority of treatment for packet filtering.

(Security ACLs are different from the location policy on a RoamAbout Switch which helps you locally control user access. For location policy commands, see Chapter 8, **AAA Commands**.)

This chapter presents security ACL commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear security acl	14-2
clear security acl map	14-4
commit security acl	14-6
rollback security acl	14-8
set security acl	14-9
set security acl map	14-14
set security acl hit-sample-rate	14-16
show security acl	14-17
show security acl editbuffer	14-18
show security acl hits	14-19
show security acl info	14-20
show security acl map	14-22
show security acl resource-usage	14-23

clear security acl

Clears a specified security ACL, an access control entry (ACE), or all security ACLs, from the edit buffer. When used with the command **commit security acl**, clears the ACE from the running configuration.

Syntax

clear security acl {*acl-name* | **all**} [*editbuffer-index*]

Parameters

acl-name	Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
all	Clears all security ACLs.
editbuffer-index	Number that indicates which access control entry (ACE) in the security ACL to clear. If you do not specify an ACE, all ACEs are cleared from the ACL.

Defaults

None.

Mode

Enabled.

Usage

This command deletes security ACLs only in the edit buffer. You must use the **commit security acl** command with this command to delete the ACL or ACE from the running configuration and nonvolatile storage.

The **clear security acl** command deletes a security ACL, but does not stop its current filtering function if the ACL is mapped to any virtual LANs (VLANs), ports, or virtual ports, or if the ACL is applied in a Filter-Id attribute to an authenticated user or group of users with current sessions.

Example

The following commands display the current security ACL configuration, clear *acl_133* in the edit buffer, commit the deletion to the running configuration, and redisplay the ACL configuration to show that it no longer contains *acl_133*:

```
RBT-8100# show security acl info all
ACL information for all
set security acl ip acl_133 (hits #1 0)
----------------------------------------------------------
1. deny IP source IP 192.168.1.6 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
----------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
----------------------------------------------------------
```

```
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
RBT-8100# clear security acl acl_133
RBT-8100# commit security acl acl_133
configuration accepted
RBT-8100# show security acl info all
ACL information for all
set security acl ip acl_134 (hits #3 0)
----------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
----------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

Related Commands

- clear security acl map on page 14-4
- commit security acl on page 14-6
- set security acl on page 14-9
- show security acl info on page 14-20

clear security acl map

Deletes the mapping between a security ACL and a virtual LAN (VLAN), one or more physical ports, or a virtual port. Or deletes all ACL maps to VLANs, ports, and virtual ports on a RoamAbout Switch.

Note: Security ACLs are applied to users or groups dynamically via the Filter-Id attribute. To delete a security ACL from a user or group in the local RoamAbout Switch database, use the command **clear user attr**, **clear mac-user attr**, **clear usergroup attr**, or **clear mac-usergroup attr**. To delete a security ACL from a user or group on an external RADIUS server, see the documentation for your RADIUS server.

Syntax

clear security acl map {*acl-name* | **all**} {**vlan** *vlan-id* | **port** *port-list* [**tag** *tag-value*] | **dap** *dap-num*} {**in** | **out**}

Parameters

acl-name	Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
all	Removes security ACL mapping from all physical ports, virtual ports, and VLANs on a RoamAbout Switch.
vlan *vlan-id*	VLAN name or number. MSS removes the security ACL from the specified VLAN.
port *port-list*	Port list. MSS removes the security ACL from the specified RoamAbout Switch physical port or ports.
tag *tag-value*	Tag value that identifies a virtual port in a VLAN. Specify a value from 1 through 4095. MSS removes the security ACL from the specified virtual port.
dap *dap-num*	One or more Distributed APs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS removes the security ACL from the specified Distributed APs.
in	Removes the security ACL from traffic coming *into* the RoamAbout Switch.
out	Removes the security ACL from traffic going *out of* the RoamAbout Switch.

Defaults

None.

Mode

Enabled.

Usage

To clear a security ACL map, type the name of the ACL with the VLAN, physical port or ports, virtual port tag, or Distributed AP and the direction of the packets to stop filtering. This command deletes the ACL mapping, but not the ACL.

Examples

To clear the mapping of security ACL *acljoe* from port 4 for incoming packets, type the following command:

```
RBT-8100# clear security acl map acljoe port 4 in
clear mapping accepted
```

To clear all physical ports, virtual ports, and VLANs on a RoamAbout Switch of the ACLs mapped for incoming and outgoing traffic, type the following command:

```
RBT-8100# clear security acl map all
success: change accepted.
```

Related Commands

- clear security acl on page 14-2
- set security acl map on page 14-14
- show security acl map on page 14-22

commit security acl

Saves a security ACL, or all security ACLs, in the edit buffer to the running configuration and nonvolatile storage on the RoamAbout Switch. Or, when used with the **clear security acl** command, **commit security acl** deletes a security ACL, or all security ACLs, from the running configuration and nonvolatile storage.

Syntax

commit security acl {*acl-name* | **all**}

Parameters

acl-name	Name of an existing security ACL to commit. ACL names must start with a letter and are case-insensitive.
all	Commits all security ACLs in the edit buffer.

Defaults

None.

Mode

Enabled.

Usage

Use the **commit security acl** command to save security ACLs into, or delete them from, the permanent configuration. Until you commit the creation or deletion of a security ACL, it is stored in an edit buffer and is not enforced. After you commit a security ACL, it is removed from the edit buffer.

A single **commit security acl all** command commits the creation and/or deletion of whatever **show security acl info all editbuffer** shows to be currently stored in the edit buffer.

Example

The following commands commit all the security ACLs in the edit buffer to the configuration, display a summary of the committed ACLs, and show that the edit buffer has been cleared:

```
RBT-8100# commit security acl all
configuration accepted
RBT-8100# show security acl
ACL table
ACL                     Type  Class   Mapping
----------------------  ----  ------  -------
acl_123                 IP    Static
acl_124                 IP    Static
RBT-8100# show security acl info all editbuffer
acl editbuffer information for all
```

Related Commands

- clear security acl on page 14-2
- rollback security acl on page 14-8
- set security acl on page 14-9
- show security acl on page 14-17
- show security acl info on page 14-20

rollback security acl

Clears changes made to the security ACL edit buffer since it was last saved. The ACL is rolled back to its state after the last **commit security acl** command was entered. All uncommitted ACLs in the edit buffer are cleared.

Syntax

rollback security acl {*acl-name* | **all**}

Parameters

acl-name	Name of an existing security ACL to roll back. ACL names must start with a letter and are case-insensitive.
all	Rolls back all security ACLs in the edit buffer, clearing all uncommitted ACEs.

Defaults

None.

Mode

Enabled.

Example

The following commands show the edit buffer before a rollback, clear any changes in the edit buffer to security *acl_122*, and show the edit buffer after the rollback:

```
RBT-8100# show security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl_122 (ACEs 3, add 3, del 0, modified 0)
------------------------------------------------------------
1. permit IP source IP 20.0.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 20.0.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
RBT-8100# rollback security acl acl_122
RBT-8100# show security acl info all editbuffer
ACL edit-buffer information for all
```

Related Commands

show security acl on page 14-17

set security acl

In the edit buffer, creates a security access control list (ACL), adds one access control entry (ACE) to a security ACL, and/or reorders ACEs in the ACL. The ACEs in an ACL filter IP packets by source IP address, a Layer 4 protocol, or IP, ICMP, TCP, or UDP packet information.

Syntax

By source address:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} *source-ip-addr mask* [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

By Layer 4 protocol:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} *protocol-number* {*source-ip-addr mask destination-ip-addr mask*} [**precedence** *precedence*] [**tos** *tos*] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

By IP packets:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **ip** {*source-ip-addr mask destination-ip-addr mask*} [**precedence** *precedence*] [**tos** *tos*] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

By ICMP packets:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **icmp** {*source-ip-addr mask destination-ip-addr mask*} [**type** *icmp-type*] [**code** *icmp-code*] [**precedence** *precedence*] [**tos** *tos*] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

By TCP packets:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **tcp** {*source-ip-addr mask* [*operator port* [*port2*]] *destination-ip-addr mask* [*operator port* [*port2*]]} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

By UDP packets:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **udp** {*source-ip-addr mask* [*operator port* [*port2*]] *destination-ip-addr mask* [*operator port* [*port2*]]} [**precedence** *precedence*] [**tos** *tos*] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

Parameters

acl-name	Security ACL name. ACL names must be unique within the RoamAbout Switch, must start with a letter, and are case-insensitive. Specify an ACL name of up to 32 of the following characters: • Letters *a* through *z* and *A* through *Z* • Numbers 0 through 9 • Hyphen (-), underscore (_), and period (.) Enterasys Networks recommends that you do not use the same name with different capitalizations for ACLs. For example, do not configure two separate ACLs with the names *acl_123* and *ACL_123*. **Note:** In an ACL name, do *not* include the term **all**, **default-action**, **map**, **help**, or **editbuffer**.
permit	Allows traffic that matches the conditions in the ACE.
cos *cos*	For permitted packets, a class-of-service (CoS) level for packet handling. Specify a value from 0 through 7: • **1** or **2**—Background. Packets are queued in AP forwarding queue 4. • **0** or **3**—Best effort. Packets are queued in AP forwarding queue 3. • **4** or **5**—Video. Packets are queued in AP forwarding queue 2. Use CoS level 4 or 5 for voice over IP (VoIP) packets other than SpectraLink Voice Priority (SVP). • **6** or **7**—Voice. Packets are queued in AP forwarding queue 1. Use 6 or 7 only for VoIP phones that use SVP, not for other types of traffic
deny	Blocks traffic that matches the conditions in the ACE.
protocol	IP protocol by which to filter packets: • **ip** • **tcp** • **udp** • **icmp** • A protocol number between 0 and 255. (For a complete list of IP protocol names and numbers, see www.iana.org/assignments/protocol-numbers.)
source-ip-addr mask	IP address and wildcard mask of the network or host *from* which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see "Wildcard Masks" on page 1-3.

operator port [port2]	Operand and port number(s) for matching TCP or UDP packets to the number of the source or destination port on *source-ip-addr* or *destination-ip-addr*. Specify one of the following operands and the associated port: • **eq**—Packets are filtered for only *port* number. • **gt**—Packets are filtered for all ports that are greater than *port* number. • **lt**—Packets are filtered for all ports that are less than *port* number. • **neq**—Packets are filtered for all ports except *port* number. • **range**—Packets are filtered for ports in the range between *port* and *port2*. To specify a port range, enter two port numbers. Enter the lower port number first, followed by the higher port number. (For a complete list of TCP and UDP port numbers, see www.iana.org/assignments/port-numbers.)
destination-ip-addr mask	IP address and wildcard mask of the network or host *to* which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see "Wildcard Masks" on page 1-3.
type *icmp-type*	Filters ICMP messages by type. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)
code *icmp-code*	For ICMP messages filtered by type, additionally filters ICMP messages by code. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)
precedence *precedence*	Filters packets by precedence level. Specify a value from 0 through 7: • **0**—routine precedence • **1**—priority precedence • **2**—immediate precedence • **3**—flash precedence • **4**—flash override precedence • **5**—critical precedence • **6**—internetwork control precedence • **7**—network control precedence
tos *tos*	Filters packets by type of service (TOS) level. Specify one of the following values, or any sum of these values up to 15. For example, a **tos** value of **9** filters packets with the TOS levels minimum delay (**8**) and minimum monetary cost (**1**). • **8**—minimum delay • **4**—maximum throughput • **2**—maximum reliability • **1**—minimum monetary cost • **0**—normal

established	For TCP packets only, applies the ACE only to established TCP sessions and not to new TCP sessions.
before *editbuffer-index*	Inserts the new ACE in front of another ACE in the security ACL. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use **show security acl editbuffer**.)
modify *editbuffer-index*	Replaces an ACE in the security ACL with the new ACE. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use **show security acl editbuffer**.)
hits	Tracks the number of packets that are filtered based on a security ACL, for all mappings.

Defaults

By default, permitted packets are classified based on DSCP value, which is converted into an internal CoS value in the switch's CoS map. The packet is then marked with a DSCP value based on the internal CoS value. If the ACE contains the **cos** option, this option overrides the switch's CoS map and marks the packet based on the ACE.

Mode

Enabled.

Notes:

- The **any** option is supported for the source or destination IP address and mask. This option is equivalent to **0.0.0.0 255.255.255.255**.
- The **any** option is shown in the configuration file as **0.0.0.0 255.255.255.255**, regardless of whether you specify **any** or **0.0.0.0 255.255.255.255** when you configure the ACE.

Note: The **dscp** *codepoint* is added. This option enables you to filter based on a packet's Differentiated Services Code Point (DSCP) value.

Usage

The RoamAbout Switch does not apply security ACLs until you activate them with the **commit security acl** command and map them to a VLAN, port, or virtual port, or to a user. If the RoamAbout Switch is reset or restarted, any ACLs in the edit buffer are lost.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

The order of security ACEs in a security ACL is important. Once an ACL is active, its ACEs are checked according to their order in the ACL. If an ACE criterion is met, its action takes place and any ACEs that follow are ignored.

ACEs are listed in the order in which you create them, unless you move them. To position security ACEs within a security ACL, use **before** *editbuffer-index* and **modify** *editbuffer-index*.

Examples

The following command adds an ACE to security *acl_123* that permits packets from IP address 192.168.1.11/24 and counts the hits:

```
RBT-8100# set security acl ip acl_123 permit 192.168.1.11 0.0.0.255 hits
```

The following command adds an ACE to *acl_123* that denies packets from IP address 192.168.2.11:

```
RBT-8100# set security acl ip acl_123 deny 192.168.2.11 0.0.0.0
```

The following command creates *acl_125* by defining an ACE that denies TCP packets from source IP address 192.168.0.1 to destination IP address 192.168.0.2 for established sessions only, and counts the hits:

```
RBT-8100# set security acl ip acl_125 deny tcp 192.168.0.1 0.0.0.0 192.168.0.2
0.0.0.0 established hits
```

The following command adds an ACE to *acl_125* that denies TCP packets from source IP address 192.168.1.1 to destination IP address 192.168.1.2, on destination port 80 only, and counts the hits:

```
RBT-8100# set security acl ip acl_125 deny tcp 192.168.1.1 0.0.0.0 192.168.1.2
0.0.0.0 eq 80 hits
```

Finally, the following command commits the security ACLs in the edit buffer to the configuration:

```
RBT-8100# commit security acl all
configuration accepted
```

Related Commands

- clear security acl on page 14-2
- commit security acl on page 14-6
- show security acl on page 14-17

set security acl map

Assigns a committed security ACL to a VLAN, physical port or ports, virtual port, or Distributed AP on the RoamAbout Switch.

Note: To assign a security ACL to a user or group in the local RoamAbout Switch database, use the command **set user attr**, **set mac-user attr**, **set usergroup attr**, or **set mac-usergroup attr** with the Filter-Id attribute. To assign a security ACL to a user or group with Filter-Id on a RADIUS server, see the documentation for your RADIUS server.

Syntax

set security acl map *acl-name* {**vlan** *vlan-id* | **port** *port-list* [**tag** *tag-list*] | **dap** *dap-num*} {**in** | **out**}

Parameters

acl-name	Name of an existing security ACL to map. ACL names start with a letter and are case-insensitive.
vlan *vlan-id*	VLAN name or number. MSS assigns the security ACL to the specified VLAN.
port *port-list*	Port list. MSS assigns the security ACL to the specified physical RoamAbout Switch port or ports.
tag *tag-list*	One or more values that identify a virtual port in a VLAN. Specify a single tag value from 1 through 4095. Or specify a comma-separated list of values, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified virtual port or ports.
dap *dap-num*	One or more Distributed APs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified Distributed APs.
in	Assigns the security ACL to traffic coming *into* the RoamAbout Switch .
out	Assigns the security ACL to traffic coming *from* the RoamAbout Switch .

Defaults

None.

Mode

Enabled.

Usage

Before you can map a security ACL, you must use the **commit security acl** command to save the ACL in the running configuration and nonvolatile storage.

For best results, map only one input security ACL and one output security ACL to each VLAN, physical port, virtual port, or Distributed AP to filter a flow of packets. If more than one security ACL filters the same traffic, MSS applies only the first ACL match and ignores any other matches.

Example

The following command maps security ACL *acl_133* to port 4 for incoming packets:

```
RBT-8100 set security acl map acl_133 port 4 in
success: change accepted.
```

Related Commands

- clear security acl map on page 14-4
- commit security acl on page 14-6
- set mac-user attr on page 8-44
- set mac-usergroup attr on page 8-50
- set security acl on page 14-9
- set user attr on page 8-57
- set user group on page 8-58
- show security acl map on page 14-22

set security acl hit-sample-rate

Specifies the time interval, in seconds, at which the packet counter for each security ACL is sampled for display. The counter counts the number of packets filtered by the security ACL—or "hits."

Syntax

set security acl hit-sample-rate *seconds*

Parameters

seconds	Number of seconds between samples. A sample rate of 0 (zero) disables the sample process.

Defaults

By default, the hits are not sampled.

Mode

Enabled.

Usage

To view counter results for a particular ACL, use the **show security acl info** *acl-name* command. To view the hits for all security ACLs, use the **show security acl hits** command.

Example

The first command sets MSS to sample ACL hits every 15 seconds. The second and third commands display the results. The results show that 916 packets matching security *acl_153* were sent since the ACL was mapped.

```
RBT-8100# set security acl hit-sample-rate 15
RBT-8100# show security acl info acl_153
ACL information for acl_153
set security acl ip acl_153 (hits #3 916)
-------------------------------------------------------
1. permit IP source IP 20.1.1.1 0.0.0.0 destination IP any enable-hits
RBT-8100# show security acl hits
ACL hit counters
Index Counter              ACL-name
----- -------------------- -----------
    1                    0 acl_2
    2                    0 acl_175
    3                  916 acl_153
```

Related Commands

- show security acl hits on page 14-19
- show security acl info on page 14-20

show security acl

Displays a summary of the security ACLs that are mapped.

Syntax

show security acl

Defaults

None.

Mode

Enabled.

Usage

This command lists only the ACLs that have been mapped to something (a user, or VLAN, or port, and so on). To list all committed ACLs, use the **show security acl info** command. To list ACLs that have not yet been committed, use the **show security acl editbuffer** command.

Example

To display a summary of the mapped security ACLs on an RoamAbout Switch, type the following command:

```
RBT-8100# show security acl
ACL table
ACL                          Type Class  Mapping
---------------------------- ---- ------ -------
acl_123                      IP   Static Port 2 In
acl_133                      IP   Static Port 4 In
acl_124                      IP   Static
```

Related Commands

- clear security acl on page 14-2
- commit security acl on page 14-6
- set security acl on page 14-9
- show security acl editbuffer on page 14-18
- show security acl info on page 14-20

show security acl editbuffer

Displays a summary of the security ACLs that have not yet been committed to the configuration.

Syntax

show security acl [**info all**] **editbuffer**

Parameters

info all	Displays the ACEs in each uncommitted ACL. Without this option, only the ACE names are listed.

Defaults

None.

Mode

Enabled.

Examples

To view a summary of the security ACLs in the edit buffer, type the following command:

```
RBT-8100# show security acl editbuffer
ACL edit-buffer table
ACL                          Type Status
---------------------------- ---- --------------
acl_111                      IP   Not committed
acl-a                        IP   Not committed
```

To view details about these uncommitted ACLs, type the following command.

```
RBT-8100# show security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl-111 (ACEs 3, add 3, del 0, modified 2)
---------------------------------------------------
 1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP any
 3. deny SRC source IP 192.168.253.1 0.0.0.255
set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
---------------------------------------------------
 1. permit SRC source IP 192.168.1.1 0.0.0.0
```

Related Commands

- clear security acl on page 14-2
- commit security acl on page 14-6
- set security acl on page 14-9
- show security acl on page 14-17
- show security acl info on page 14-20

show security acl hits

Displays the number of packets filtered by security ACLs (“hits”) on the RoamAbout Switch. Each time a packet is filtered by a security ACL, the hit counter increments.

Syntax

show security acl hits

Parameters

None.

Defaults

None.

Mode

Enabled.

Usage

For MSS to count hits for a security ACL, you must specify **hits** in the **set security acl** commands that define ACE rules for the ACL.

Example

To display the security ACL hits on a RoamAbout Switch, type the following command:

```
RBT-8100# show security acl hits
ACL hit-counters
Index Counter              ACL-name
----- -------------------- --------
    1                    0 acl_2
    2                    0 acl_175
    3                  916 acl_123
```

Related Commands

- set security acl hit-sample-rate on page 14-16
- set security acl on page 14-9

show security acl info

Displays the contents of a specified security ACL or all security ACLs that are committed—saved in the running configuration and nonvolatile storage—or the contents of security ACLs in the edit buffer before they are committed.

Syntax

show security acl info [*acl-name* | **all**] [**editbuffer**]

Parameters

acl-name	Name of an existing security ACL to display. ACL names must start with a letter and are case-insensitive.
all	Displays the contents of all security ACLs.
editbuffer	Displays the contents of the specified security ACL or all security ACLs that are stored in the edit buffer after being created with **set security acl**. If you do not use this parameter, only committed ACLs are shown.

Defaults

None.

Mode

Enabled.

Example

To display the contents of all security ACLs committed on a RoamAbout Switch, type the following command:

```
RBT-8100# show security acl info all
ACL information for all
set security acl ip acl_123 (hits #5 462)
----------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
----------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
----------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

The following command displays the contents of *acl_123* in the edit buffer, including the committed ACE rules 1 and 2 and the uncommitted rule 3:

```
RBT-8100# show security acl info acl_123 editbuffer
ACL edit-buffer information for acl_123
set security acl ip acl_123 (ACEs 3, add 3, del 0, modified 0)
----------------------------------------------------------
```

```
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
```

Related Commands

- clear security acl on page 14-2
- commit security acl on page 14-6
- set security acl on page 14-9

show security acl map

Displays the VLANs, ports, and virtual ports on the RoamAbout Switch to which a security ACL is assigned.

Syntax

show security acl map *acl-name*

Parameters

acl-name	Name of an existing security ACL for which to show static mapping. ACL names must start with a letter and are case-insensitive.

Defaults

None.

Mode

Enabled.

Example

The following command displays the port to which security ACL *acl_111* is mapped:

```
RBT-8100# show security acl map acl_111
ACL acl_111 is mapped to:
Port 4 in
```

Related Commands

- clear security acl map on page 14-4
- set security acl map on page 14-14
- show security acl on page 14-17

show security acl resource-usage

Displays statistics about the resources used by security ACL filtering on the RoamAbout Switch.

Syntax

```
show security acl resource-usage
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Usage

Use this command with the help of the Enterasys Global Technical Assistance Center (GTAC) to diagnose an ACL resource problem. (To contact GTAC, see "Getting Help" on page xxiii.)

To display security ACL resource usage, type the following command:

```
RBT-8100# show security acl resource-usage
ACL resources


Classifier tree counters
------------------------
  Number of rules           : 2
  Number of leaf nodes      : 1
  Stored rule count         : 2
  Leaf chain count          : 1
  Longest leaf chain        : 2
  Number of non-leaf nodes  : 0
  Uncompressed Rule Count   : 2
  Maximum node depth        : 1
  Sub-chain count           : 0
  PSCBs in primary memory   : 0 (max: 512)
  PSCBs in secondary memory : 0 (max: 9728)
  Leaves in primary         : 2 (max: 151)
Leaves in secondary       : 0 (max 12096)
  Sum node depth            : 1
Information on Network Processor status
---------------------------------------
  Fragmentation control     : 0
  UC switchdest             : 0
ACL resources
  Port number               : 0
  Number of action types    : 2
  LUdef in use              : 5
```

```
Default action pointer    : c8007dc
L4 global                 : True
No rules                  : False
Non-IP rules              : False
Root in first             : True
Static default action     : False
No per-user (MAC) mapping : True
Out mapping               : False
In mapping                : True
No VLAN or PORT mapping   : False
No VPORT mapping          : True
```

Table 14-1 explains the fields in the **show security acl resource-usage** output.

Table 14-1 show security acl resource-usage Output

Field	Description
Number of rules	Number of security ACEs currently mapped to ports or VLANs.
Number of leaf nodes	Number of security ACL data entries stored in the rule tree.
Stored rule count	Number of security ACEs stored in the rule tree.
Leaf chain count	Number of chained security ACL data entries stored in the rule tree.
Longest leaf chain	Longest chain of security ACL data entries stored in the rule tree.
Number of non-leaf nodes	Number of nodes with no data entries stored in the rule tree.
Uncompressed Rule Count	Number of security ACEs stored in the rule tree, including duplicates—ACEs in ACLs applied to multiple ports, virtual ports, or VLANs.
Maximum node depth	Number of data elements in the rule tree, from the root to the furthest data entry (leaf).
Sub-chain count	Sum of action types represented in all security ACL data entries.
PSCBs in primary memory	Number of pattern search control blocks (PSCBs) stored in primary node memory.
PSCBs in secondary memory	Number of PSCBs stored in secondary node memory.
Leaves in primary	Number of security ACL data entries stored in primary leaf memory.
Leaves in secondary	Number of ACL data entries stored in secondary leaf memory.
Sum node depth	Total number of security ACL data entries.
Fragmentation control	Control value for handling fragmented IP packets. **Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
UC switchdest	Control value for handling fragmented IP packets. **Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.

Table 14-1 show security acl resource-usage Output (continued)

Field	Description
Port number	Control value for handling fragmented IP packets. **Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
Number of action types	Number of actions that can be performed by ACLs. This value is always 2, because ACLs can either *permit* or *deny*.
LUdef in use	Number of the lookup definition (LUdef) table currently in use for packet handling.
Default action pointer	Memory address used for packet handling, from which default action data is obtained when necessary.
L4 global	Security ACL mapping on the RoamAbout Switch: • True—Security ACLs are mapped. • False—No security ACLs are mapped.
No rules	Security ACE rule mapping on the RoamAbout Switch: • True—No security ACEs are mapped. • False—Security ACEs are mapped.
Non-IP rules	Non-IP security ACE mapping on the RoamAbout Switch: • True—Non-IP security ACEs are mapped. • False—Only IP security ACEs are mapped. **Note:** The current MSS version supports security ACEs for IP only.
Root in first	Leaf buffer allocation: • True—Enough primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves. • False—Insufficient primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves.
Static default action	Definition of a default action: • True—A default action types is defined. • False—No default action type is defined.
No per-user (MAC) mapping	Per-user application of a security ACL with the Filter-Id attribute, on the RoamAbout Switch: • True—No security ACLs are applied to users. • False—Security ACLs are applied to users.
Out mapping	Application of security ACLs to outgoing traffic on the RoamAbout Switch: • True—Security ACLs are mapped to outgoing traffic. • False—No security ACLs are mapped to outgoing traffic.
In mapping	Application of security ACLs to incoming traffic on the RoamAbout Switch: • True—Security ACLs are mapped to incoming traffic. • False—No security ACLs are mapped to incoming traffic.

Table 14-1 show security acl resource-usage Output (continued)

Field	Description
No VLAN or PORT mapping	Application of security ACLs to RoamAbout Switch VLANs or ports on the RoamAbout Switch: • True—No security ACLs are mapped to VLANs or ports. • False—Security ACLs are mapped to VLANs or ports.
No VPORT mapping	Application of security ACLs to RoamAbout Switch virtual ports on the RoamAbout Switch: • True—No security ACLs are mapped to virtual ports. • False—Security ACLs are mapped to virtual ports.

15

Cryptography Commands

A digital certificate is a form of electronic identification for computers. The RoamAbout Switch requires digital certificates to authenticate its communications to RoamAbout Switch Manager and WebView, to WebAAA clients, and to Extensible Authentication Protocol (EAP) clients for which the RoamAbout switch performs all EAP processing. Certificates can be generated on the RoamAbout or obtained from a certificate authority (CA). Keys contained within the certificates allow the RoamAbout, its servers, and its wireless clients to exchange information secured by encryption.

Notes:

- If the switch does not already have certificates, MSS automatically generates the missing ones the first time you boot using MSS Version 4.2 or later. You do not need to install certificates unless you want to replace the ones automatically generated by MSS. (For more information, see the "Certificates Automatically Generated by MSS" section in the "Managing Keys and Certificates" chapter of the *RoamAbout Mobility System Software Configuration Guide*.)
- Before installing a new certificate, verify with the **show timedate** and **show timezone** commands that the RoamAbout Switch is set to the correct date, time, and time zone. Otherwise, certificates might not be installed correctly.

This chapter presents cryptography commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
crypto ca-certificate	15-2
crypto certificate	15-4
crypto generate key	15-6
crypto generate request	15-7
crypto generate self-signedweb	15-9
crypto otp	15-11
crypto pkcs12	15-13
show crypto ca-certificate	15-15
show crypto certificate	15-17
show crypto key domain	15-18
show crypto key ssh	15-19

crypto ca-certificate

Installs a certificate authority's own PKCS #7 certificate into the RoamAbout Switch certificate and key storage area.

Syntax

crypto ca-certificate {**admin** | **eap** | **web**} *PEM-formatted-certificate*

Parameters

admin	Stores the certificate authority's certificate that signed the administrative certificate for the RoamAbout Switch. The administrative certificate authenticates the RoamAbout Switch to RASM or WebView.
eap	Stores the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the RoamAbout. The EAP certificate authenticates the RAS to 802.1X supplicants (clients).
web	Stores the certificate authority's certificate that signed the certificate for the RoamAbout Switch. The Web certificate authenticates the RoamAbout Switch to clients who use Web Authentication.
PEM-formatted-certificate	ASCII text representation of the certificate authority PKCS #7 certificate, consisting of up to 5120 characters that you have obtained from the certificate authority.

Defaults

None.

Mode

Enabled.

Usage

The Privacy-Enhanced Mail protocol (PEM) format is used for representing a PKCS #7 certificate in ASCII text. PEM uses base64 encoding to convert the certificate to ASCII text, then puts the encoded text between the following delimiters:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

To use this command, you must already have obtained a copy of the certificate authority's certificate as a PKCS #7 object file. Then do the following:

1. Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
2. Enter the **crypto ca-certificate** command on the CLI command line.
3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

Example

The following command adds the certificate authority's certificate to RoamAbout Switch certificate and key storage:

```
RBT-8100# crypto ca-certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIDwDCCA2qgAwIBAgIQL2jvuu4PO5FAQCyewU3ojANBgkqhkiG9wOBAQUFADCB
mzerMClaweVQQTTooewi\wpoer0QWNFNkj90044mbdrl1277SWQ8G7DiwYUtrqoQplKJvxz
.....
Lm8wmVYxP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

Related Commands

show crypto ca-certificate on page 15-15

crypto certificate

Installs one of the RoamAbout switch's PKCS #7 certificates into the certificate and key storage area on the RoamAbout. The certificate, which is issued and signed by a certificate authority, authenticates the RoamAbout Switch either to RASM or WebView, or to 802.1X supplicants (clients).

Syntax

crypto certificate {**admin** | **eap** | **web**} *PEM-formatted certificate*

Parameters

admin	Stores the certificate authority's administrative certificate, which authenticates the RoamAbout to RASM or WebView.
eap	Stores the certificate authority's Extensible Authentication Protocol (EAP) certificate, which authenticates the RoamAbout to 802.1X supplicants (clients).
web	Stores the certificate authority's certificate, which authenticates the RAS to clients who use Web Authentication
PEM-formatted certificate	ASCII text representation of the PKCS #7 certificate, consisting of up to 5120 characters, that you have obtained from the certificate authority.

Defaults

None.

Mode

Enabled.

Usage

To use this command, you must already have generated a certificate request with the **crypto generate request** command, sent the request to the certificate authority, and obtained a signed copy of the RoamAbout certificate as a PKCS #7 object file. Then do the following:

1. Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
2. Enter the **crypto certificate** command on the CLI command line.
3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

The RoamAbout Switch verifies the validity of the public key associated with this certificate before installing it, to prevent a mismatch between the RoamAbout switch's private key and the public key in the installed certificate.

Example

The following command installs a certificate:

```
RBT-8100# crypto certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIBdTCP3wIBADA2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQOExGjAYBgNVBAMU
EXR1Y2hwdWJzQHRycHouY29tMIGfMAOGCSqGSIb3DQEBAQAA4GNADCBiQKBgQC4
.....
2L8Q9tk+G2As84QYLm8wmVY>xP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

Related Commands

- crypto generate request on page 15-7
- crypto generate self-signedweb on page 15-9

crypto generate key

Generates an RSA public-private encryption key pair that is required for a Certificate Signing Request (CSR) or a self-signed certificate. For SSH, generates an authentication key.

Syntax

```
crypto generate key {admin | domain | eap | ssh | web}{128 | 512 | 1024 | 2048}
```

Parameters

admin	Generates an administrative key pair for authenticating the RoamAbout Switch to RASM or WebView.
domain	Generates a key pair for authenticating management traffic exchanged by RoamAbout switches within a Mobility Domain.
eap	Generates an EAP key pair for authenticating the RoamAbout Switch to 802.1X supplicants (clients).
ssh	Generates a key pair for authenticating the RoamAbout Switch to Secure Shell (SSH) clients.
web	Generates an administrative key pair for authenticating the RoamAbout Switch to Web Authenticating clients.
128 | **512** | **1024** | **2048**	Length of the key pair in bits. The minimum key length for SSH is **1024**. The length **128** applies only to **domain** and is the only valid option for it.

Defaults

None.

Mode

Enabled.

Usage

You can overwrite a key by generating another key of the same type.

SSH requires an SSH authentication key, but you can allow MSS to generate it automatically. The first time an SSH client attempts to access the SSH server on a RoamAbout Switch, the switch automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

Example

To generate an administrative key for use with RASM, type the following command:

```
RBT-8100# crypto generate key admin 1024
key pair generated
```

Related Commands

show crypto key ssh on page 15-19

crypto generate request

Generates a Certificate Signing Request (CSR). This command outputs a PEM-formatted PKCS #10 text string that you can cut and paste to another location for delivery to a certificate authority.

This command generates either an administrative CSR for use with RASM and WebView, or an EAP CSR for use with 802.1X clients.

Syntax

crypto generate request {**admin** | **eap** | **web**}

Parameters

admin	Generates a request for an administrative certificate to authenticate the RoamAbout Switch to RASM or WebView.
eap	Generates a request for an EAP certificate to authenticate the RoamAbout Switch to 802.1X supplicants (clients).
web	Generates a request for a certificate to authenticate the RoamAbout Switch to Web Authenticating clients.

After typing the command, you are prompted for the following variables:

Country Name *string*	(Optional) Specify the abbreviation for the country in which the RoamAbout Switch is operating, in 2 alphanumeric characters with no spaces.
State Name *string*	(Optional) Specify the name of the state, in up to 64 alphanumeric characters. Spaces are allowed.
Locality Name *string*	(Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
Organizational Name *string*	(Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
Organizational Unit *string*	(Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
Common Name *string*	Specify a unique name for the RoamAbout Switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.
Email Address *string*	(Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
Unstructured Name *string*	(Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

Defaults

None.

Mode

Enabled.

Usage

To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Enter **crypto generate request admin**, **crypto generate request eap**, or **crypto generate request web authentication** and press Enter. When you are prompted, type the identifying values in the fields, or press Enter if the field is optional. You must enter a common name for the RoamAbout Switch.

This command outputs a PKCS #10 text string in Privacy-Enhanced Mail protocol (PEM) format that you paste to another location for submission to the certificate authority. You then send the request to the certificate authority to obtain a signed copy of the RoamAbout certificate as a PKCS #7 object file.

Example

To request an administrative certificate from a certificate authority, type the following command:

```
RBT-8100# crypto generate request admin
Country Name: US
State Name: CA
Locality Name: Pleasanton
Organizational Name: Enterasys
Organizational Unit: ENG
Common Name: ENG
Email Address: admin@example.com
Unstructured Name: admin
CSR for admin is
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQCAQAwezELMAkGA1UEBhMCdXMxCzAJBgNVBAgTAmNhMQswCQYDVQQH
EwJjYTELMAkGA1UEChMCY2ExCzAJBgNVBAsTAmNhMQswCQYDVQQDEwJjYTEYMBYG
CSqGSIb3DQEJARYJY2FAY2EuY29tMREwDwYJKoZIhvcNAQkCEwJjYTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA1zatpYStOjHMa0QJmWHeZPPFGQ9kBEimJKPG
bznFjAC780GcZtnJPGqnMnOKj/4NdknonT6NdCd2fBdGbuEFGNMNgZMYKGcV2JIu
M32SvpSEOEnMYuidkEzqLQol621vh67RM1KTMECM6uCBBROq6XNypIHn1gtrrpL/
LhyGTWUCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAHK5z2kfjBbV/F0b0MyC5S7K
htsw7T4SwmCij55qfUHxsRelggYcw6vJtr57jJ7wFfsMd8C50NcbJLF1nYC9OKkB
hW+5gDPAOZdOnnr591XKz3Zzyvyrktv00rcld8Fo2RtTQ3AOT9cUZqJVelO85GXJ
-----END CERTIFICATE REQUEST-----
```

Related Commands

- crypto certificate on page 15-4
- crypto generate key on page 15-6

crypto generate self-signedweb

Generates a self-signed certificate for either an administrative certificate for use with RASM or an EAP certificate for use with 802.1X wireless users.

Syntax

crypto generate self-signed {**admin** | **eap** | **web**}

Parameters

admin	Generates an administrative certificate to authenticate the RoamAbout Switch to RASM or WebView.
eap	Generates an EAP certificate to authenticate the RoamAbout Switch to 802.1X supplicants (clients).
web	Generates a webcertificate to authenticate the RoamAbout Switch to Web Authenticating clients.

After type the command, you are prompted for the following variables:

Country Name *string*	(Optional) Specify the abbreviation for the country in which the RoamAbout Switch is operating, in 2 alphanumeric characters with no spaces.
State Name *string*	(Optional) Specify the abbreviation for the name of the state, in 2 alphanumeric characters with no spaces.
Locality Name *string*	(Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
Organizational Name *string*	(Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
Organizational Unit *string*	(Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
Common Name *string*	Specify a unique name for the RoamAbout Switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required. **Note:** If you are generating a certificate for Web Authenticationweb, use a common name that looks like a domain name (two or more strings connected by dots, with no spaces). For example, use *common.name* instead of *common name*. The string is not required to be an actual domain name. It simply needs to be formatted like one.
Email Address *string*	(Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
Unstructured Name *string*	(Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

Defaults

None.

Mode

Enabled.

Usage

To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Example

To generate a self-signed administrative certificate, type the following command:

```
RBT-8100# crypto generate self-signed admin
Country Name:
State Name:
Locality Name:
Organizational Name:
Organizational Unit:
Common Name: RBT1@example.com
Email Address:
Unstructured Name:
```

Related Commands

- crypto certificate on page 15-4
- crypto generate key on page 15-6

crypto otp

Sets a one-time password (OTP) for use with the **crypto pkcs12** command.

Syntax

crypto otp {**admin** | **eap** | **web**} *one-time-password*

Parameters

admin	Creates a one-time password for installing a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the RoamAbout Switch to RASM or WebView.
eap	Creates a one-time password for installing a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the RoamAbout Switch to 802.1X supplicants (clients).
web	Creates a one-time password for installing a PKCS #12 object file for a certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the RoamAbout Switch to Web Authenticating clients.
one-time-password	Password of at least 1 alphanumeric character, with no spaces, for clients other than Microsoft Windows clients. The password must be the same as the password protecting the PKCS #12 object file. **Note:** On a RoamAbout Switch that handles communications to and from Microsoft Windows clients, use a one-time password of 31 characters or fewer. The following characters *cannot* be used as part of the one-time password of a PKCS #12 file: • Quotation marks (" ") • Question mark (?) • Ampersand (&)

Defaults

None.

Mode

Enabled.

Usage

The password allows the public-private key pair and certificate to be installed together from the same PKCS #12 object file. MSS erases the one-time password after processing the **crypto pkcs12** command or when you reboot the RoamAbout Switch.

Enterasys Networks recommends that you create a password that is memorable to you but is not subject to easy guesses or a dictionary attack. For best results, create a password of alphanumeric uppercase and lowercase characters.

Example

The following command creates the one-time password *hap9iN#ss* for installing an EAP certificate and key pair:

```
RBT-8100# crypto generate otp eap hap9iN#ss
OTP set
```

Related Commands

crypto pkcs12 on page 15-13

crypto pkcs12

Unpacks a PKCS #12 object file into the certificate and key storage area on the RoamAbout Switch. This object file contains a public-private key pair, a RoamAbout certificate signed by a certificate authority, and the certificate authority's certificate.

Syntax

crypto pkcs12 {**admin** | **eap** | **web**} *file-location-url*

Parameters

admin	Unpacks a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the RoamAbout Switch to RASM or WebView.
eap	Unpacks a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the RoamAbout Switch to 802.1X supplicants (clients).
web	Unpacks a PKCS #12 object file for a certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the RoamAbout Switch to Web Authenticating clients.
file-location-url	Location of the PKCS #12 object file to be installed. Specify a location of between 1 and 128 alphanumeric characters, with no spaces.

Defaults

The password you enter with the **crypto otp** command must be the same as the one protecting the PKCS #12 file.

Mode

Enabled.

Usage

To use this command, you must have already created a one-time password with the **crypto otp** command.

You must also have the PKCS #12 object file available. You can download a PKCS #12 object file via TFTP from a remote location to the local nonvolatile storage system on the RoamAbout Switch.

Example

The following commands copy a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—from a TFTP server to nonvolatile storage on the RoamAbout Switch, create the one-time password *hap9iN#ss*, and unpack the PKCS #12 file:

```
RBT-8100# copy tftp://192.168.253.1/2048full.p12 2048full.p12
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
RBT-8100# crypto otp eap hap9iN#ss
OTP set
RBT-8100# crypto pkcs12 eap 2048full.p12
Unwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
```

Related Commands

crypto otp on page 15-11

show crypto ca-certificate

Displays information about the certificate authority's PEM-encoded PKCS #7 certificate.

Syntax

```
show crypto ca-certificate {admin | eap | web}
```

Parameters

admin	Displays information about the certificate authority's certificate that signed the administrative certificate for the RoamAbout Switch. The administrative certificate authenticates the RoamAbout Switch to RASM or WebView.
eap	Displays information about the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the RoamAbout Switch. The EAP certificate authenticates the RAS to 802.1X supplicants (clients).
web	Displays information about the certificate authority's certificate that signed the certificate for the RoamAbout Switch. The certificate authenticates the RoamAbout Switch to Web Authenticating clients.

Defaults

None.

Mode

Enabled.

Example

To display information about the certificate of a certificate authority, type the following command:

```
RBT-8100# show crypto ca-certificate
```

Table 15-1 describes the fields in the display.

Table 15-1 Output for show crypto ca-certificate

Output	What It Displays...
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

Related Commands

- crypto ca-certificate on page 15-2
- show crypto certificate on page 15-17

show crypto certificate

Displays information about one of the cryptographic certificates installed on the RoamAbout Switch.

Syntax

```
show crypto certificate {admin | eap | web}
```

Parameters

admin	Displays information about the administrative certificate that authenticates the RoamAbout Switch to RASM or WebView.
eap	Displays information about the EAP certificate that authenticates the RoamAbout Switch to 802.1X supplicants (clients).
web	Displays information about the certificate that authenticates the RoamAbout Switch to Web Authenticating clients.

Defaults

None.

Mode

Enabled.

Usage

You must have generated a self-signed certificate or obtained a certificate from a certificate authority before displaying information about the certificate.

Example

To display information about a cryptographic certificate, type the following command:

```
RBT-8100# show crypto certificate eap
```

Table 15-2 describes the fields of the display.

Table 15-2 Output for crypto certificate

Output	What It Displays...
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

Related Commands

- crypto generate self-signedweb on page 15-9
- show crypto ca-certificate on page 15-15

show crypto key domain

Displays the checksum (also called a *fingerprint*) of the public key used to authenticate management traffic between RoamAbout Switches.

Syntax

```
show crypto key domain
```

Defaults

None.

Mode

Enabled.

Example

To display the fingerprint for RoamAbout Switch to RoamAbout Switch security, type the following command:

```
RBT-8100# show crypto key domain
Domain public key:
e6:43:91:e2:b3:53:ed:46:76:5f:f0:96:3a:3b:86:d3
```

Related Commands

crypto generate key on page 15-6

show crypto key ssh

Displays SSH authentication key information. This command displays the checksum (also called a *fingerprint*) of the public key. When you connect to the RoamAbout Switch with an SSH client, you can compare the SSH key checksum displayed by the RoamAbout Switch with the one displayed by the client to verify that you really are connected to the RoamAbout Switch and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

Syntax

show crypto key ssh

Defaults

None.

Mode

Enabled.

Example

To display SSH key information, type the following command:

```
RBT-8100# show crypto key ssh
ec:6f:56:7f:d1:fd:c0:28:93:ae:a4:f9:7c:f5:13:04
```

Related Commands

crypto generate key on page 15-6

16

RADIUS and Server Groups Commands

Use RADIUS commands to set up communication between a RoamAbout switch and groups of up to four RADIUS servers for remote authentication, authorization, and accounting (AAA) of administrators and network users. This chapter presents RADIUS commands alphabetically.

Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear radius	16-2
clear radius client system-ip	16-4
clear radius proxy client	16-5
clear radius proxy port	16-6
clear radius server	16-7
clear server group	16-8
set radius	16-9
set radius client system-ip	16-11
set radius proxy client	16-12
set radius proxy port	16-13
set radius server	16-14
set server group	16-16
set server group load-balance	16-17

(For information about RADIUS attributes, see the RADIUS appendix in the *RoamAbout Mobility System Software Configuration Guide*.)

clear radius

Resets parameters that were globally configured for RADIUS servers to their default values.

Syntax

```
clear radius {deadtime | key | retransmit | timeout}
```

Parameters

deadtime	Number of minutes to wait after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server.
key	Password (shared secret key) used to authenticate to the RADIUS server.
retransmit	Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable.
timeout	Number of seconds to wait for the RADIUS server to respond before retransmitting.

Defaults

Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The RoamAbout switch does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

Mode

Enabled.

Usage

To override the globally set values on a particular RADIUS server, use the **set radius server** command.

Example

To reset all global RADIUS parameters to their factory defaults, type the following commands:

```
RBT-8100# clear radius deadtime
success: change accepted.
RBT-8100# clear radius key
success: change accepted.
RBT-8100# clear radius retransmit
success: change accepted.
RBT-8100# clear radius timeout
success: change accepted.
```

Related Commands

- set radius on page 16-9
- set radius server on page 16-14
- show aaa on page 8-62

clear radius client system-ip

Removes the RoamAbout switch's system IP address from use as the permanent source address in RADIUS client requests from the switch to its RADIUS server(s).

Syntax

```
clear radius client system-ip
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Usage

The **clear radius client system-ip** command causes the RoamAbout switch to use the IP address of the interface through which it sends a RADIUS client request as the source IP address. The RoamAbout switch selects a source interface address based on information in its routing table as the source address for RADIUS packets leaving the switch.

Example

To clear the system IP address as the permanent source address for RADIUS client requests, type the following command:

```
RBT-8100# clear radius client system-ip
success: change accepted.
```

Related Commands

- set radius client system-ip on page 16-11
- show aaa on page 8-62

clear radius proxy client

Removes RADIUS proxy client entries for third-party APs.

Syntax

```
clear radius proxy client all
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following command clears all RADIUS proxy client entries from the switch:

```
RBT-8100# clear radius proxy client all
success: change accepted.
```

Related Commands

set radius proxy client on page 16-12

clear radius proxy port

Removes RADIUS proxy ports configured for third-party APs.

Syntax

```
clear radius proxy port all
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following command clears all RADIUS proxy port entries from the switch:

```
RBT-8100# clear radius proxy port all
success: change accepted.
```

Related Commands

set radius proxy port on page 16-13

clear radius server

Removes the named RADIUS server from the RoamAbout switch configuration.

Syntax

clear radius server *server-name*

Parameters

server-name	Name of a RADIUS server configured to perform remote AAA services for the RoamAbout switch.

Defaults

None.

Mode

Enabled.

Example

The following command removes the RADIUS server *rs42* from a list of remote AAA servers:

```
RBT-8100# clear radius server rs42
success: change accepted.
```

Related Commands

- set radius server on page 16-14
- show aaa on page 8-62

clear server group

Removes a RADIUS server group from the configuration, or disables load balancing for the group.

Syntax

clear server group *group-name* [**load-balance**]

Parameters

group-name	Name of a RADIUS server group configured to perform remote AAA services for RoamAbout switches.
load-balance	Ability of group members to share demand for services among servers.

Defaults

None.

Mode

Enabled.

Usage

Deleting a server group removes the server group from the configuration. However, the members of the server group remain.

Example

To remove the server group *sg-77* type the following command:

```
RBT-8100# clear server group sg-77
success: change accepted.
```

To disable load balancing in a server group *shorebirds*, type the following command:

```
RBT-8100# set server group shorebirds load-balance disable
success: change accepted.
```

Related Commands

set server group on page 16-16

set radius

Configures global defaults for RADIUS servers that do not explicitly set these values themselves. By default, the RoamAbout switch automatically sets all these values except the password (key).

Syntax

```
set radius {deadtime minutes | encrypted-key string | key string |
retransmit number | timeout seconds}
```

Parameters

deadtime *minutes*	Number of minutes the RoamAbout switch waits after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. You can specify from 0 to 1440 minutes.
encrypted-key *string*	Password (shared secret key) used to authenticate to the RADIUS server, entered in its encrypted form. You must provide the same encrypted password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs. MSS does not encrypt the string you enter, and instead displays the string in **show config** and **show aaa** output exactly as you entered it. **Note:** Use this option only if you are entering the key in its encrypted form. To enter the key in unencrypted form, use the **key** *string* option instead.
key *string*	Password (shared secret key) used to authenticate to the RADIUS server, entered in its unencrypted form. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs. MSS encrypts the displayed form of the string in **show config** and **show aaa** output. **Note:** Use this option only if you are entering the key in its unencrypted form. To enter the key in encrypted form, use the **encrypted-key** *string* option instead. .
retransmit *number*	Number of transmission attempts the RoamAbout switch makes before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
timeout *seconds*	Number of seconds the RoamAbout switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535.

Defaults

Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The RoamAbout switch does not designate unresponsive RADIUS servers as unavailable.)
- **encrypted-key**—No key
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

Mode

Enabled.

Usage

You can specify only one parameter per command line.

Example

The following commands sets the dead time to 5 minutes, the RADIUS key to *goody*, the number of retransmissions to 1, and the timeout to 21 seconds on all RADIUS servers connected to the RoamAbout switch:

```
RBT-8100# set radius deadtime 5
success: change accepted.
RBT-8100# set radius key goody
success: change accepted.
RBT-8100# set radius retransmit 1
success: change accepted.
RBT-8100# set radius timeout 21
success: change accepted.
```

Related Commands

- clear radius server on page 16-7
- set radius server on page 16-14
- show aaa on page 8-62

set radius client system-ip

Causes all RADIUS requests to be sourced from the IP address specified by the **set system ip-address** command, providing a permanent source IP address for RADIUS packets sent from the RoamAbout switch.

Syntax

```
set radius client system-ip
```

Defaults

None.

If you do not use this command, RADIUS packets leaving the RoamAbout switch have the source IP address of the outbound interface, which can change as routing conditions change.

Mode

Enabled.

Usage

The RoamAbout switch system IP address must be set before you use this command.

Example

The following command sets the RoamAbout switch system IP address as the address of the RADIUS client:

```
RBT-8100# set radius client system-ip
success: change accepted.
```

Related Commands

- clear radius client system-ip on page 16-4
- set system ip-address on page 3-20

set radius proxy client

Adds a RADIUS proxy entry for a third-party AP. The proxy entry specifies the IP address of the AP and the UDP port on which the RoamAbout switch listens for RADIUS traffic from the AP.

Syntax

set radius proxy client address *ip-address* [**port** *udp-port-number*] **key** *string*

Parameters

address *ip-address*	IP address of the third-party AP. Enter the address in dotted decimal notation.
port *udp-port-number*	UDP port on which the RoamAbout switch listens for RADIUS traffic from the AP.
key *string*	Password (shared secret key) the RoamAbout switch uses to authenticate and encrypt RADIUS communication.

Defaults

The default UDP port number is 1812.

Mode

Enabled.

Usage

AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the Enterasys Networks *Mobility System Software Configuration Guide*.

Example

The following command configures a RADIUS proxy entry for a third-party AP RADIUS client at 10.20.20.9, sending RADIUS traffic to the default UDP port 1812 on the RoamAbout switch:

```
RBT-8100# set radius proxy client address 10.20.20.9 key radkey1
success: change accepted.
```

Related Commands

- clear radius proxy client on page 16-5
- set authentication proxy on page 8-37
- set radius proxy port on page 16-13

set radius proxy port

Configures the RoamAbout switch port connected to a third-party AP as a RADIUS proxy for the SSID supported by the AP.

Syntax

set radius proxy port *port-list* [**tag** *tag-value*] **ssid** *ssid-name*

Parameters

port *port-list*	RoamAbout switch port(s) connected to the third-party AP.
tag *tag-value*	802.1Q tag value in packets sent by the third-party AP for the SSID.
ssid *ssid-name*	SSID supported by the third-party AP.

Defaults

None.

Mode

Enabled.

Usage

AAA for third-party AP users has additional configuration requirements. See the "Configuring AAA for Users of Third-Party APs" section in the "Configuring AAA for Network Users" chapter of the *RoamAbout Mobility System Software Configuration Guide*.

Enter a separate command for each SSID, and its tag value, you want the RoamAbout switch to support.

Example

The following command maps SSID *mycorp* to packets received on port 3 or 4, using 802.1Q tag value 104:

```
RBT-8100# set radius proxy port 3-4 tag 104 ssid mycorp
success: change accepted.
```

Related Commands

- clear radius proxy port on page 16-6
- clear authentication proxy on page 8-8
- set radius proxy client on page 16-12

set radius server

Configures RADIUS servers and their parameters. By default, the RoamAbout switch automatically sets all these values except the password (key).

Syntax

set radius server *server-name* [**address** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**deadtime** *minutes*] [[**key** *string*] | [**encrypted-key** *string*]] [**author-password** *password*]

Parameters

server-name	Unique name for this RADIUS server. Enter an alphanumeric string of up to 32 characters, with no blanks.
address *ip-address*	IP address of the RADIUS server. Enter the address in dotted decimal notation.
auth-port *port-number*	UDP port that the RoamAbout switch uses for authentication and authorization.
acct-port *port-number*	UDP port that the RoamAbout switch uses for accounting.
timeout *seconds*	Number of seconds the RoamAbout switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535 seconds.
retransmit *number*	Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
deadtime *minutes*	Number of minutes the RoamAbout switch waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server. Specify between 0 (zero) and 1440 minutes (24 hours). A zero value causes the switch to identify unresponsive servers as available.
key *string* | **encrypted-key** *string*	Password (shared secret key) the RoamAbout Switch uses to authenticate to RADIUS servers. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs. • Use the **key** option to enter the string in its unencrypted form. MSS encrypts the displayed form of the string in **show config** and **show aaa** output. • To enter the string in its encrypted form instead, use the **encrypted-key** option. MSS does not encrypt the string you enter, and instead displays the string exactly as you enter it.
author-password *password*	Password used for authorization to a RADIUS server for MAC authentication. The client's MAC address is sent as the username and the **author-password** string is sent as the password. Specify a password of up to 64 alphanumeric characters with no spaces or tabs.

Defaults

Default values are listed below:

- **auth-port**—UDP port 1812
- **acct-port**—UDP port 1813
- **timeout**—5 seconds
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **deadtime**—0 (zero) minutes (The RoamAbout switch does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **encrypted-key**—No key
- **author-password**—nopassword

Mode

Enabled.

Usage

For a given RADIUS server, the first instance of this command must set both the server name and the IP address and can include any or all of the other optional parameters. Subsequent instances of this command can be used to set optional parameters for a given RADIUS server.

To configure the server as a remote authenticator for the RoamAbout switch, you must add it to a server group with the **set server group** command.

Do not use the same name for a RADIUS server and a RADIUS server group.

Example

To set a RADIUS server named RS42 with IP address 198.162.1.1 to use the default accounting and authorization ports with a timeout interval of 30 seconds, two transmit attempts, 5 minutes of dead time, a key string of *keys4u*, and the default authorization password of *nopassword*, type the following command:

```
RBT-8100# set radius server RS42 address 198.162.1.1 timeout 30 retransmit 2
deadtime 5 key keys4U
```

Related Commands

- set authentication admin on page 8-27
- set authentication console on page 8-29
- set authentication dot1x on page 8-31
- clear authentication mac on page 8-7
- set authentication web on page 8-38
- set radius on page 16-9
- set server group on page 16-16
- show aaa on page 8-62

set server group

Configures a group of one to four RADIUS servers.

Syntax

set server group *group-name* **members** *server-name1* [*server-name2*] [*server-name3*] [*server-name4*]

Parameters

group-name	Server group name of up to 32 characters, with no spaces or tabs.
members *server-name1*	The names of one or more configured RADIUS servers. You can enter up to four server names.
server-name2	
server-name3	
server-name4	

Defaults

None.

Mode

Enabled.

Usage

You must assign all group members simultaneously, as shown in the example. To enable load balancing, use **set server group load-balance enable**.

Do not use the same name for a RADIUS server and a RADIUS server group.

Example

To set server group *shorebirds* with members *heron*, *egret*, and *sandpiper*, type the following command:

```
RBT-8100# set server group shorebirds members heron egret sandpiper
success: change accepted.
```

Related Commands

- clear server group on page 16-8
- set server group load-balance on page 16-17
- show aaa on page 8-62

set server group load-balance

Enables or disables load balancing among the RADIUS servers in a server group.

Syntax

set server group *group-name* **load-balance** {**enable** | **disable**}

Parameters

group-name	Server group name of up to 32 characters.
load-balance **enable** | **disable**	Enables or disables load balancing of authentication requests among the servers in the group.

Defaults

Load balancing is disabled by default.

Mode

Enabled.

Usage

You can optionally enable load balancing after assigning the server group members. If you configure load balancing, MSS sends each AAA request to a separate server, starting with the first one on the list and skipping unresponsive servers. If no server in the group responds, MSS moves to the next method configured with **set authentication** and **set accounting**.

In contrast, if load balancing is *not* configured, MSS always begins with the first server in the list and sends unfulfilled requests to each subsequent server in the group before moving on to the next configured AAA method.

Example

To enable load balancing between the members of server group *shorebirds*, type the following command:

```
RBT-8100# set server group shorebirds load-balance enable
success: change accepted.
```

To disable load balancing between *shorebirds* server group members, type the following command:

```
RBT-8100# set server group shorebirds load-balance disable
success: change accepted.
```

Related Commands

- clear server group on page 16-8
- clear radius server on page 16-7
- set server group on page 16-16
- show aaa on page 8-62

17

802.1X Management Commands

Use 802. IEEE X management commands to modify the default settings for IEEE 802.1X sessions on a RAS. For best results, change the settings only if you are aware of a problem with the RoamAbout switch's 802.1X performance.

This chapter presents 802.1X commands alphabetically. Use the following table to locate commands in this chapter. For information about configuring 802.1X commands for user authentication, see Chapter 8, **AAA Commands**.

Caution: 802.1X parameter settings are global for all SSIDs configured on the switch.

For information about...	Refer to page...
clear dot1x bonded-period	17-3
clear dot1x max-req	17-4
clear dot1x port-control	17-5
clear dot1x quiet-period	17-6
clear dot1x reauth-max	17-7
clear dot1x reauth-period	17-8
clear dot1x timeout auth-server	17-9
clear dot1x timeout supplicant	17-10
clear dot1x tx-period	17-11
set dot1x authcontrol	17-12
set dot1x bonded-period	17-13
set dot1x key-tx	17-14
set dot1x max-req	17-15
set dot1x port-control	17-16
set dot1x quiet-period	17-17
set dot1x reauth	17-18
set dot1x reauth-max	17-19
set dot1x reauth-period	17-20
set dot1x timeout auth-server	17-21

For information about...	Refer to page...
set dot1x timeout supplicant	17-22
set dot1x tx-period	17-23
set dot1x wep-rekey	17-24
set dot1x wep-rekey-period	17-25
show dot1x	17-26

clear dot1x bonded-period

Resets the Bonded Auth period to its default value.

Syntax

```
clear dot1x max-req
```

Parameters

None.

Defaults

The default bonded authentication period is 0 seconds.

Mode

Enabled.

Example

To reset the Bonded period to its default, type the following command:

```
RBT-8100# clear dot1x bonded-period
success: change accepted.
```

Related Commands

- set dot1x bonded-period on page 17-13
- show dot1x on page 17-26

clear dot1x max-req

Resets to the default setting the number of Extensible Authentication Protocol (EAP) requests that the RoamAbout switch retransmits to a supplicant (client).

Syntax

```
clear dot1x max-req
```

Parameters

None.

Defaults

The default number is 20.

Mode

Enabled.

Example

To reset the number of 802.1X requests the RoamAbout switch can send to the default setting, type the following command:

```
RBT-8100# clear dot1x max-req
success: change accepted.
```

Related Commands

- set dot1x max-req on page 17-15
- show dot1x on page 17-26

clear dot1x port-control

Resets all wired authentication ports on the RoamAbout switch to default 802.1X authentication.

Syntax

clear dot1x port-control

Defaults

By default, all wired authentication ports are set to **auto** and they process authentication requests as determined by the **set authentication dot1X** command.

Mode

Enabled.

Usage

This command is overridden by the **set dot1x authcontrol** command. The **clear dot1x port-control** command returns port control to the method configured. This command applies only to wired authentication ports.

Example

Type the following command to reset the wired authentication port control:

```
RBT-8100# clear dot1x port-control
success: change accepted.
```

Related Commands

- set dot1x port-control on page 17-16
- show dot1x on page 17-26

clear dot1x quiet-period

Resets the quiet period after a failed authentication to the default setting.

Syntax

```
clear dot1x quiet-period
```

Parameters

None.

Defaults

The default is 60 seconds.

Mode

Enabled.

Example

Type the following command to reset the 802.1X quiet period to the default:

```
RBT-8100# clear dot1x quiet-period
success: change accepted.
```

Related Commands

- set dot1x quiet-period on page 17-17
- show dot1x on page 17-26

clear dot1x reauth-max

Resets the maximum number of reauthorization attempts to the default setting.

Syntax

```
clear dot1x reauth-max
```

Parameters

None.

Defaults

The default is 2 attempts.

Mode

Enabled.

Example

Type the following command to reset the maximum number of reauthorization attempts to the default:

```
RBT-8100# clear dot1x reauth-max
success: change accepted.
```

Related Commands

- set dot1x reauth-max on page 17-19
- show dot1x on page 17-26

clear dot1x reauth-period

Resets the time period that must elapse before a reauthentication attempt, to the default time period.

Syntax

```
clear dot1x reauth-period
```

Parameters

None.

Defaults

The default is 3600 seconds (1 hour).

Mode

Enabled.

Example

Type the following command to reset the default reauthentication time period:

```
RBT-8100# clear dot1x reauth-period
success: change accepted.
```

Related Commands

- set dot1x reauth-period on page 17-20
- show dot1x on page 17-26

clear dot1x timeout auth-server

Resets to the default setting the number of seconds that must elapse before the RoamAbout switch times out a request to a RADIUS server.

Syntax

```
clear dot1x timeout auth-server
```

Parameters

None.

Defaults

The default is 30 seconds.

Mode

Enabled.

Example

To reset the default timeout for requests to an authentication server, type the following command:

```
RBT-8100# clear dot1x timeout auth-server
success: change accepted.
```

Related Commands

- set dot1x timeout auth-server on page 17-21
- show dot1x on page 17-26

clear dot1x timeout supplicant

Resets to the default setting the number of seconds that must elapse before the RoamAbout switch times out an authentication session with a supplicant (client).

Syntax

```
clear dot1x timeout supplicant
```

Parameters

None.

Defaults

The default for the authentication timeout sessions is 30 seconds.

Mode

Enabled.

Example

Type the following command to reset the timeout period for an authentication session:

```
RBT-8100# clear dot1x timeout supplicant
success: change accepted.
```

Related Commands

- set dot1x timeout supplicant on page 17-22
- show dot1x on page 17-26

clear dot1x tx-period

Resets to the default setting the number of seconds that must elapse before the RoamAbout switch retransmits an EAP over LAN (EAPoL) packet.

Syntax

```
clear dot1x tx-period
```

Parameters

None.

Defaults

The default is 5 seconds.

Mode

Enabled.

Example

Type the following command to reset the EAPoL retransmission time:

```
RBT-8100# clear dot1x tx-period
success: change accepted.
```

Related Commands

- set dot1x tx-period on page 17-23
- show dot1x on page 17-26

set dot1x authcontrol

Provides a global override mechanism for 802.1X authentication configuration on wired authentication ports.

Syntax

```
set dot1x authcontrol {enable | disable}
```

Parameters

enable	Allows all wired authentication ports running 802.1X to use the authentication specified per port by the **set dot1X port-control** command.
disable	Forces all wired authentication ports running 802.1X to unconditionally accept all 802.1X authentication attempts with an EAP Success message (ForceAuth).

Defaults

By default, authentication control for individual wired authentication is enabled.

Mode

Enabled.

Usage

This command applies only to wired authentication ports.

Example

To enable per-port 802.1X authentication on wired authentication ports, type the following command:

```
RBT-8100# set dot1x authcontrol enable
success: dot1x authcontrol enabled.
```

Related Commands

- set dot1x port-control on page 17-16
- show dot1x on page 17-26

set dot1x bonded-period

Changes the Bonded Auth™ (bonded authentication) period. The *Bonded Auth period* is the number of seconds MSS allows a Bonded Auth user to reauthenticate.

Syntax

set dot1x bonded-period *seconds*

Parameters

seconds	Number of seconds MSS retains session information for an authenticated machine while waiting for a client to (re)authenticate on the same machine. You can change the bonded authentication period to a value from 1 to 300 seconds.

Defaults

The default bonded period is 0 seconds, which disables the feature.

Mode

Enabled.

Usage

Normally, the Bonded Auth period needs to be set only if the network has Bonded Auth clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

Example

To set the bonded authentication period to 60 seconds, type the following command:

```
RBT-8100# set dot1x bonded-period 60
success: change accepted.
```

Related Commands

- clear dot1x bonded-period on page 17-3
- show dot1x on page 17-26

set dot1x key-tx

Enables or disables the transmission of encryption key information to the supplicant (client) in EAP over LAN (EAPoL) key messages, after authentication is successful.

Syntax

set dot1x key-tx {**enable** | **disable**}

Parameters

enable	Enables transmission of encryption key information to clients.
disable	Disables transmission of encryption key information to clients.

Defaults

Key transmission is enabled by default.

Mode

Enabled.

Example

Type the following command to enable key transmission:

```
RBT-8100# set dot1x key-tx enable
success: dot1x key transmission enabled.
```

Related Commands

show dot1x on page 17-26

set dot1x max-req

Sets the maximum number of times the RoamAbout switch retransmits an EAP request to a supplicant (client) before ending the authentication session.

Syntax

set dot1x max-req *number-of-retransmissions*

Parameters

number-of-retransmissions	Specify a value between 0 and 10.

Defaults

The default number of EAP retransmissions is 2.

Mode

Enabled.

Usage

To support SSIDs that have both 802.1X and static WEP clients, MSS sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

Example

Type the following command to set the maximum number of EAP request retransmissions to three attempts:

```
RBT-8100# set dot1x max-req 3
success: dot1x max request set to 3.
```

Related Commands

- clear dot1x max-req on page 17-4
- show dot1x on page 17-26

set dot1x port-control

Determines the 802.1X authentication behavior on individual wired authentication ports or groups of ports.

Syntax

set dot1x port-control {**forceauth** | **forceunauth** | **auto**} *port-list*

Parameters

forceauth	Forces the specified wired authentication port(s) to *unconditionally authorize* all 802.1X authentication attempts, with an EAP success message.
forceunauth	Forces the specified wired authentication port(s) to *unconditionally reject* all 802.1X authentication attempts with an EAP failure message.
auto	Allows the specified wired authentication ports to process 802.1X authentication normally as determined for the user by the **set authentication dot1X** command.
port-list	One or more wired authentication ports for which to set 802.1X port control.

Defaults

By default, wired authentication ports are set to auto.

Mode

Enabled.

Usage

This command affects only wired authentication ports.

Example

The following command forces port 19 to unconditionally accept all 802.1X authentication attempts:

```
RBT-8100# set dot1x port-control forceauth 19
success: authcontrol for 19 is set to FORCE-AUTH.
```

Related Commands

- show port status on page 4-31
- show dot1x on page 17-26

set dot1x quiet-period

Sets the number of seconds a RoamAbout switch remains quiet and does not respond to a supplicant after a failed authentication.

Syntax

set dot1x quiet-period *seconds*

Parameters

seconds	Specify a value between 0 and 65,535.

Defaults

The default is 60 seconds.

Mode

Enabled.

Example

Type the following command to set the quiet period to 90 seconds:

```
RBT-8100# set dot1x quiet-period 90
success: dot1x quiet period set to 90.
```

Related Commands

- clear dot1x quiet-period on page 17-6
- show dot1x on page 17-26

set dot1x reauth

Determines whether the RoamAbout switch allows the reauthentication of supplicants (clients).

Syntax

```
set dot1x reauth {enable | disable}
```

Parameters

enable	Permits reauthentication.
disable	Denies reauthentication.

Defaults

Reauthentication is enabled by default.

Mode

Enabled.

Example

Type the following command to enable reauthentication of supplicants (clients):

```
RBT-8100# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

Related Commands

- set dot1x reauth-max on page 17-19
- set dot1x reauth-period on page 17-20
- show dot1x on page 17-26

set dot1x reauth-max

Sets the number of reauthentication attempts that the RoamAbout switch makes before the supplicant (client) becomes unauthorized.

Syntax

set dot1x reauth-max *number-of-attempts*

Parameters

number-of-attempts	Specify a value between 1 and 10.

Defaults

The default number of reauthentication attempts is 2.

Mode

Enabled.

Usage

If the number of reauthentications for a wired authentication client is greater than the maximum number of reauthentications allowed, MSS sends an EAP failure packet to the client and removes the client from the network. However, MSS does not remove a wireless client from the network under these circumstances.

Example

Type the following command to set the number of authentication attempts to 8:

```
RBT-8100# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```

Related Commands

- clear dot1x reauth-max on page 17-7
- show dot1x on page 17-26

set dot1x reauth-period

Sets the number of seconds that must elapse before the RoamAbout switch attempts reauthentication.

Syntax

set dot1x reauth-period *seconds*

Parameters

seconds	Specify a value between 60 (1 minute) and 1,641,600 (19 days).

Defaults

The default is 3600 seconds (1 hour).

Mode

Enabled.

Example

Type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
RBT-8100# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

Related Commands

- clear dot1x reauth-period on page 17-8
- show dot1x on page 17-26

set dot1x timeout auth-server

Sets the number of seconds that must elapse before the RoamAbout switch times out a request to a RADIUS authentication server.

Syntax

set dot1x timeout auth-server *seconds*

Parameters

seconds	Specify a value between 1 and 65,535.

Defaults

The default is 30 seconds.

Mode

Enabled.

Example

Type the following command to set the authentication server timeout to 60 seconds:

```
RBT-8100# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```

Related Commands

- clear dot1x timeout auth-server on page 17-9
- show dot1x on page 17-26

set dot1x timeout supplicant

Sets the number of seconds that must elapse before the RoamAbout switch times out an authentication session with a supplicant (client).

Syntax

set dot1x timeout supplicant *seconds*

Parameters

seconds	Specify a value between 1 and 65,535.

Defaults

The default is 30 seconds.

Mode

Enabled.

Example

Type the following command to set the number of seconds for authentication session timeout to 300:

```
RBT-8100# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

Related Commands

- clear dot1x timeout auth-server on page 17-9
- show dot1x on page 17-26

set dot1x tx-period

Sets the number of seconds that must elapse before the RoamAbout switch retransmits an EAPoL packet.

Syntax

set dot1x tx-period *seconds*

Parameters

seconds	Specify a value between 1 and 65,535.

Defaults

The default is 5 seconds.

Mode

Enabled.

Example

Type the following command to set the number of seconds before the RoamAbout switch retransmits an EAPoL packet to 300:

```
RBT-8100# set dot1x tx-period 300
success: dot1x tx-period set to 300.
```

Related Commands

- clear dot1x tx-period on page 17-11
- show dot1x on page 17-26

set dot1x wep-rekey

Enables or disables Wired Equivalency Privacy (WEP) rekeying for broadcast and multicast encryption keys.

Syntax

```
set dot1X wep-rekey {enable | disable}
```

Parameters

enable	Causes the broadcast and multicast keys for WEP to be rotated at an interval set by the **set dot1x wep-rekey-period** for each radio, associated VLAN, and encryption type. The RoamAbout switch generates the new broadcast and multicast keys and pushes the keys to the clients via EAPoL key messages.
disable	WEP broadcast and multicast keys are never rotated.

Defaults

WEP key rotation is enabled, by default.

Mode

Enabled.

Usage

Reauthentication is *not* required for WEP key rotation to take place. Broadcast and multicast keys are always rotated at the same time, so all members of a given radio, VLAN, or encryption type receive the new keys at the same time.

Example

Type the following command to disable WEP key rotation:

```
RBT-8100# set dot1x wep-rekey disable
success: wep rekeying disabled
```

Related Commands

- set dot1x wep-rekey-period on page 17-25
- show dot1x on page 17-26

set dot1x wep-rekey-period

Sets the interval for rotating the WEP broadcast and multicast keys.

Syntax

set dot1x wep-rekey-period *seconds*

Parameters

seconds	Specify a value between 30 and 1,641,600 (19 days).

Defaults

The default is 1800 seconds (30 minutes).

Mode

Enabled.

Example

Type the following command to set the WEP-rekey period to 300 seconds:

```
RBT-8100# set dot1x wep-rekey-period 300
success: dot1x wep-rekey-period set to 300
```

Related Commands

- set dot1x wep-rekey on page 17-24
- show dot1x on page 17-26

show dot1x

Displays 802.1X client information for statistics and configuration settings.

Syntax

show dot1x {**clients** | **stats** | **config**}

Parameters

clients	Displays information about active 802.1X clients, including client name, MAC address, and state.
stats	Displays global 802.1X statistics associated with connecting and authenticating.
config	Displays a summary of the current configuration.

Defaults

None.

Mode

Enabled.

Example

Type the following command to display the 802.1X clients:

```
RBT-8100# show dot1x clients
MAC Address               State        Vlan             Identity
  -------------             -------      ------           ----------
00:20:a6:48:01:1f       Connecting      (unknown)
00:05:3c:07:6d:7c       Authenticated   vlan-it          EXAMPLE\jose
00:05:5d:7e:94:83       Authenticated   vlan-eng         EXAMPLE\singh
00:02:2d:86:bd:38       Authenticated   vlan-eng         bard@xmple.com
00:05:5d:7e:97:b4       Authenticated   vlan-eng         EXAMPLE\havel
00:05:5d:7e:98:1a       Authenticated   vlan-eng         EXAMPLE\nash
00:0b:be:a9:dc:4e       Authenticated   vlan-pm          xalik@xmple.com
00:05:5d:7e:96:e3       Authenticated   vlan-eng         EXAMPLE\mishan
00:02:2d:6f:44:77       Authenticated   vlan-eng         EXAMPLE\ethan
00:05:5d:7e:94:89       Authenticated   vlan-eng         EXAMPLE\fmarshall
00:06:80:00:5c:02       Authenticated   vlan-eng         EXAMPLE\bmccarthy
00:02:2d:6a:de:f2       Authenticated   vlan-pm          neailey@xmple.com
00:02:2d:5e:5b:76       Authenticated   vlan-pm          EXAMPLE\tamara
00:02:2d:80:b6:e1       Authenticated   vlan-cs          dmc@xmple.com
00:30:65:16:8d:69       Authenticated   vlan-wep         MAC authenticated
00:02:2d:64:8e:1b       Authenticated   vlan-eng         EXAMPLE\wong
```

Type the following command to display the 802.1X configuration:

```
RBT-8100# show dot1x config

802.1X user policy
                  ----------------------
```

```
        'host/bob-laptop.mycorp.com' on ssid 'mycorp' doing PASSTHRU
        'bob.mycorp.com' on ssid 'mycorp' doing PASSTHRU (bonded)

        802.1X parameter                setting
        ----------------                -------
        supplicant timeout              30
        auth-server timeout             30
        quiet period                    5
        transmit period                 5
        reauthentication period         3600
        maximum requests                2
        key transmission                enabled
        reauthentication                enabled
        authentication control          enabled
        WEP rekey period                1800
        WEP rekey                       enabled
        Bonded period                   60

        port 5, authcontrol: auto, max-sessions: 16
        port 6, authcontrol: auto, max-sessions: 1
        port 7, authcontrol: auto, max-sessions: 1
        port 8, authcontrol: auto, max-sessions: 1
        port 9, authcontrol: auto, max-sessions: 1
        port 10, authcontrol: auto, max-sessions: 1
        port 11, authcontrol: auto, max-sessions: 1
        port 12, authcontrol: auto, max-sessions: 1
        port 13, authcontrol: auto, max-sessions: 1
        port 14, authcontrol: auto, max-sessions: 1
        port 15, authcontrol: auto, max-sessions: 1
        port 16, authcontrol: auto, max-sessions: 1
        port 22, authcontrol: auto, max-sessions: 16
```

Type the following command to display 802.1X statistics:

```
RBT-8100# show dot1x stats
        802.1X statistic                value
        ----------------                -----
        Enters Connecting:              709
        Logoffs While Connecting:       112
        Enters Authenticating:          467
        Success While Authenticating:   0
        Timeouts While Authenticating:  52
        Failures While Authenticating:  0
        Reauths While Authenticating:   0
        Starts While Authenticating:    31
        Logoffs While Authenticating:   0
        Starts While Authenticated:     85
        Logoffs While Authenticated:    1
        Bad Packets Received:           0
```

Table 17-1 explains the counters in the **show dot1x stats** output.

Table 17-1 Output for show dot1x stats

Output	What It Displays...
Enters Connecting	Number of times that the RoamAbout switch state transitions to the CONNECTING state from any other state.
Logoffs While Connecting	Number of times that the RoamAbout switch state transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPoL-Logoff message.
Enters Authenticating	Number of times that the state wildcard transitions.
Success While Authenticating	Number of times the RoamAbout switch state transitions from AUTHENTICATING from AUTHENTICATED, as a result of an EAP-Response/Identity message being received from the supplicant (client).
Timeouts While Authenticating	Number of times that the RoamAbout switch state wildcard transitions from AUTHENTICATING to ABORTING.
Failures While Authenticating	Number of times that the RoamAbout switch state wildcard transitions from AUTHENTICATION to HELD.
Reauths While Authenticating	Number of times that the RoamAbout switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Starts While Authenticating	Number of times that the RoamAbout switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-Start message being received from the Supplicant (client).
Logoffs While Authenticating	Number of times that the RoamAbout switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-logoff message being received from the Supplicant (client).
Bad Packets Received	Number of EAPoL packets received that have an invalid version or type.

18

Session Management Commands

Use session management commands to display and clear administrative and network user sessions. This chapter presents session management commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear sessions	18-2
clear sessions network	18-3
show sessions	18-5
show sessions network	18-7

clear sessions

Clears all administrative sessions, or clears administrative console or Telnet sessions.

Syntax

clear sessions {**admin** | **console** | **telnet** [**client** [*session-id*]]}

Parameters

admin	Clears sessions for all users with administrative access to the RoamAbout switch through a Telnet or SSH connection or a console plugged into the switch.
console	Clears sessions for all users with administrative access to the RoamAbout switch through a console plugged into the switch.
telnet	Clears sessions for all users with administrative access to the RoamAbout switch through a Telnet connection.
telnet client [*session-id*]	Clears all Telnet client sessions from the CLI to remote devices, or clears an individual session identified by session ID.

Defaults

None.

Mode

Enabled.

Example

To clear all administrator sessions type the following command:

```
RBT-8100# clear sessions admin
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative sessions through the console, type the following command:

```
RBT-8100# clear sessions console
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
To clear all administrative Telnet sessions, type the following command:
RBT-8100# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
To clear Telnet client session 0, type the following command:
RBT-8100# clear sessions telnet client 0
```

Related Commands

show sessions on page 18-5

clear sessions network

Clears all network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, virtual LAN (VLAN) or set of VLANs, or session ID.

Syntax

clear sessions network {**user** *user-glob* | **mac-addr** *mac-addr-glob* | **vlan** *vlan-glob* | **session-id** *local-session-id*}

Parameters

user *user-glob*	Clears all network sessions for a single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
mac-addr *mac-addr-glob*	Clears all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:), or use the wildcard character (*) to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 1-4.)
vlan *vlan-glob*	Clears all network sessions on a single VLAN or a set of VLANs. Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "VLAN Globs" on page 1-4.)
session-id *local-session-id*	Clears the specified 802.1X network session. To find local session IDs, use the **show sessions** command.

Defaults

None.

Mode

Enabled.

Usage

The **clear sessions network** command clears network sessions by deauthenticating and, for wireless clients, disassociating them.

Examples

To clear all sessions for MAC address 00:01:02:03:04:05, type the following command:

```
RBT-8100# clear sessions network mac-addr 00:01:02:03:04:05
```

To clear session 9, type the following command:

```
RBT-8100# clear sessions network session-id 9
SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:06:25:09:39:5d,
```

```
flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:06:25:09:39:5d)
```

To clear the session of user *Natasha*, type the following command:

```
RBT-8100# clear sessions network user Natasha
```

To clear the sessions of users whose name begins with the characters *Jo*, type the following command:

```
RBT-8100# clear sessions network user Jo*
```

To clear the sessions of all users on VLAN *red*, type the following command:

```
RBT-8100# clear sessions network vlan red
```

Related Commands

- show sessions on page 18-5
- show sessions network on page 18-7

show sessions

Displays session information and statistics for all users with administrative access to the RoamAbout switch, or for administrative users with either console or Telnet access.

Syntax

show sessions {**admin** | **console** | **telnet** [**client**]}

Parameters

admin	Displays sessions for all users with administrative access to the RoamAbout switch through a Telnet or SSH connection or a console plugged into the switch.
console	Displays sessions for all users with administrative access to the RoamAbout switch through a console plugged into the switch.
telnet	Displays sessions for all users with administrative access to the RoamAbout switch through a Telnet connection.
telnet client	Displays Telnet sessions from the CLI to remote devices.

Defaults

None.

Mode

All, except for **show sessions telnet client**, which has enabled access.

Examples

To view information about sessions of administrative users, type the following command:

```
RBT-8100> show sessions admin
Tty         Username              Time (s)    Type
-------     --------------------  --------    ----
tty0                              3644        Console
tty2        tech                  6           Telnet
tty3        sshadmin              381         SSH

3 admin sessions
```

To view information about console users' sessions, type the following command:

```
RBT-8100> show sessions console
Tty         Username              Time (s)
-------     --------------------  --------
console                           8573
1 console session
```

To view information about Telnet users sessions, type the following command:

```
RBT-8100> show sessions telnet
Tty          Username              Time (s)
-------      --------------------  --------
tty2         sea                   7395
```

To view information about Telnet client sessions, type the following command:

```
RBT-8100# show sessions telnet client
Session   Server Address    Server Port    Client Port
-------   --------------    ------------   -----------
0          192.168.1.81     23             48000
1           10.10.1.22      23             48001
```

Table 18-1 describes the fields of the **show sessions admin**, **show sessions console**, and **show sessions telnet** displays.

Table 18-2 describes the fields of the **show sessions telnet client** display.

Table 18-1 Output for show sessions admin, show sessions console, and show sessions telnet

Output	What It Displays...
Tty	The Telnet terminal number, or *console* for administrative users connected through the console port.
Username	Up to 30 characters of the name of an authenticated user.
Time(s)	Number of seconds the session has been active.
Type	Type of administrative session: • Console • SSH • Telnet

Table 18-2 Output for show sessions telnet client

Output	What It Displays...
Session	Session number assigned by MSS when the client session is established.
Server Address	IP address of the remote device.
Server Port	TCP port number of the remote device's TCP server.
Client Port	TCP port number MSS is using for the client side of the session.

Related Commands

clear sessions on page 18-2

show sessions network

Displays summary or verbose information about all network sessions, or network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, VLAN or set of VLANs, or session ID.

Syntax

show sessions network [**user** *user-glob* | **mac-addr** *mac-addr-glob* | **ssid** *ssid-name* | **vlan** *vlan-glob* | **session-id** *session-id* | **wired**] [**verbose**]

Parameters

user *user-glob*	Displays all network sessions for a single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see "User Globs" on page 1-3.)
mac-addr *mac-addr-glob*	Displays all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:). Or use the wildcard character (*) to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 1-4.)
ssid *ssid-name*	Displays all network sessions for an SSID.
vlan *vlan-glob*	Displays all network sessions on a single VLAN or a set of VLANs. Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see "VLAN Globs" on page 1-4.)
session-id *local-session-id*	Displays the specified network session. To find local session IDs, use the **show sessions** command. The **verbose** option is not available with this form of the **show sessions network** command.
wired	Displays all network sessions on wired authentication ports.
verbose	Provides detailed output for all network sessions or ones displayed by username, MAC address, or VLAN name.

Defaults

None.

Mode

All.

Usage

MSS displays information about network sessions in three types of displays. See the following tables for field descriptions.

Summary display	See Table 18-3 on page 18-10.
Verbose display	See Table 18-4 on page 18-10.
show sessions network session-id display	See Table 18-5 on page 18-13.

Examples

To display summary information for all network sessions, type **show sessions network**. For example:

```
RBT-8100> show sessions network
User                            Sess  IP or MAC         VLAN            Port/
Name                              ID  Address           Name            Radio
------------------------------ ----  ----------------- --------------- -----
EXAMPLE\Natasha                   4* 10.10.40.17        vlan-eng         3/1
host/laptop11.exmpl.com           6* 10.10.40.16        vlan-eng         3/2
nin@exmpl.com                   539* 10.10.40.17        vlan-eng         1/1
EXAMPLE\hosni                   302* 10.10.40.10        vlan-eng         3/1
                                563  00:0b:be:15:46:56  (none)           1/2
jose@exmpl.com                  380* 10.30.40.8         vlan-eng         1/1
00:30:65:16:8d:69               443* 10.10.40.19        vlan-wep         3/1
EXAMPLE\Geetha                  459* 10.10.40.18        vlan-eng         3/2
8 sessions total
```

The following command displays summary information about the sessions for MAC address 00:05:5d:7e:98:1a:

```
RBT-8100> show sessions network mac-addr 00:05:5d:7e:98:1a
User                          Sess  IP or MAC       VLAN         Port/
Name                            ID  Address         Name         Radio
---------------------------- ----  --------------- ------------ -----
EXAMPLE\Havel                 13* 10.10.10.40     vlan-eng      1/2
```

The following command displays summary information about all the sessions of users whose names begin with *E*:

```
RBT-8100> show sessions network user E*
User                          Sess  IP or MAC       VLAN         Port/
Name                            ID  Address         Name         Radio
---------------------------- ----  --------------- ------------ -----
EXAMPLE\Singh                 12* 10.10.10.30     vlan-eng      3/2
EXAMPLE\Havel                 13* 10.10.10.40     vlan-eng      1/2
2 sessions match criteria (of 3 total)
```

(Table 18-3 on page 18-10 describes the summary displays of **show sessions network** commands.)

The following command displays detailed (verbose) session information about user nin@example.com:

```
RBT-8100> show sessions network user nin@example.com verbose
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- -----
nin@example.com                  5* 10.20.30.40       vlan-eng         1/1
Client MAC: 00:02:2d:6e:ab:a5   GID: SESS-5-000430-686792-d8b3c564
State: ACTIVE                  (prev AUTHORIZED)
now on: RBT 192.168.12.7, AP/radio  1/1, AP 00:0b:0e:00:05:fe, as of 00:23:32 ago
1 sessions match criteria (of 10 total)
```

The following command displays verbose output about the sessions of all current network users:

```
RBT-8100> show sessions network verbose
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- -----
SHUTTLE2\exmpl                   6* 10.3.8.55         default          3/1
Client MAC: 00:06:25:13:08:33   GID: SESS-4-000404-98441-c807c14b
State: ACTIVE                  (prev AUTHORIZED)
now on: RBT 10.3.8.103, AP/radio  3/1, AP 00:0b:0e:ff:00:3a, as of
00:00:24 ago
  from: RBT 10.3.8.103, AP/radio  6/1, AP 00:0b:0e:00:05:d7, as of
00:01:07 ago
  from: RBT 10.3.8.103, AP/radio  3/1, AP 00:0b:0e:ff:00:3a, as of
00:01:53 ago
1 sessions total
```

(Table 18-4 on page 10 describes the additional fields of the **verbose** output of **show sessions network** commands.)

The following command displays information about network session 27:

```
RBT-8100> show sessions network session-id 27
Global Id: SESS-27-000430-835586-58dfe5a
State: ACTIVE
Port/Radio: 3/1
MAC Address: 00:00:2d:6f:44:77
User Name: EXAMPLE Natasha
IP Address: 10.10.40.17
Vlan Name: vlan-eng
Tag: 1
Session Timeout: 1800
Authentication Method: PEAP, using server 10.10.70.20
Session statistics as updated from AP:
Unicast packets in: 653
Unicast bytes in: 46211
Unicast packets out: 450
Unicast bytes out: 50478
```

```
Multicast packets in: 317
Multicast bytes in: 10144
Number of packets with encryption errors: 0
Number of bytes with encryption errors: 0
Last packet data rate: 2
Last packet signal strength: -67 dBm
Last packet data S/N ratio: 55
```

For descriptions of the fields of **show sessions network session-id** output, see Table 18-5 on page 18-13.

Table 18-3 Output for show sessions network (summary)

Output	What It Displays...
User Name	Up to 30 characters of the name of the authenticated user of this session.
Sess ID	Locally unique number that identifies this session. An asterisk (*) next to a session ID indicates that the session is fully active. .
IP or MAC Address	IP address of the session user, or the user's MAC address if the user has not yet received an IP address.
VLAN Name	Name of the VLAN associated with the session.
Port/Radio	Number of the port and radio through which the user is accessing this session.

Table 18-4 Output for Additional show sessions network verbose

Output	What It Displays...
Client MAC	MAC address of the session user.
GID	Global session ID, a unique session number within a Mobility Domain.

Table 18-4 Output for Additional show sessions network verbose (continued)

Output	What It Displays...
State	Status of the session: • AUTH, ASSOC REQ—Client is being associated by the 802.1X protocol. • AUTH AND ASSOC—Client is being associated by the 802.1X protocol, and the user is being authenticated. • AUTHORIZING—User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. • AUTHORIZED—User has been authorized by an AAA method. • ACTIVE—User's AAA attributes have been applied, and the user is active on the network. • DEASSOCIATED—One of the following: Wireless client has sent the RoamAbout switch a disassociate message. User associated with one of the current RoamAbout switch's access points has appeared at another RoamAbout switch in the Mobility Domain. • ROAMING AWAY—The RoamAbout switch has been sent a request to transfer the user, who is roaming, to another RoamAbout switch . • STATUS UPDATED—RoamAbout switch is receiving a final update from an Access Point about the user, who has roamed away. • WEB_AUTHING—User is being authenticated by WebAAA. • WIRED AUTH'ING—User is being authenticated by the 802.1X protocol on a wired authentication port. • KILLING—User's session is being cleared, because of 802.1X authentication failure, entry of a **clear** command, or some other event.
now on	IP address and port and radio numbers of the session's current RoamAbout switch , the MAC address of the Access Point, and the last update time.
from	IP address and port and radio numbers of the session's previous RoamAbout switch , the MAC address of the Access Point, and the last update time. Up to six roaming events are tracked in this display.
Host name	Host name of the user's networking device.

Table 18-4 Output for Additional show sessions network verbose (continued)

Output	What It Displays...

Vlan-Name
(and other attributes if set)
	Authorization attributes for the user and how they were assigned (the sources of the attribute values).
	For Vlan-Name, the source of the attribute value can be one of the following:
	• AAA—VLAN is from RADIUS or the local database.
	• initial-assignment—For a client that has roamed from one RoamAbout Switch to another, VLAN is the one assigned to the user on the RoamAbout Switch where the user first accessed the network. (This is the RoamAbout Switchj where the client's global session in the Mobility Domain started.)
	This authorization source (*initial-assignment*) is displayed only if the following conditions are true:
	  • The client roamed from another RoamAbout Switch.
	  • The service profile for the SSID the user is on is configured to keep the client's initial VLAN assignment. (This means the **keep-initial-vlan** option is enabled on the service profile.)
	  • The VLAN is not configured for the user on the roamed-to switch by the local database.
	  • A Location Policy on the roamed-to RoamAbout Switch does not set the VLAN.
	• location policy—Attribute value was assigned by a Location Policy.
	• service-profile—Attribute value is configured on the SSID, and was not overridden by other attribute sources (such as AAA or location policy).
	• Web Portal—Session is for a Web Portal client.

Table 18-5 Output for show sessions network session-id

Output	What It Displays...
Global Id	A unique session identifier within the Mobility Domain.
State	Status of the session: • AUTH, ASSOC REQ—Client is being associated by the 802.1X protocol. • AUTH AND ASSOC—Client is being associated by the 802.1X protocol, and the user is being authenticated. • AUTHORIZING—User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. • AUTHORIZED—User has been authorized by an AAA method. • ACTIVE—User's AAA attributes have been applied, and the user is active on the network. • DEASSOCIATED—One of the following: Wireless client has sent the RoamAbout switch a disassociate message. User associated with one of the current RoamAbout switch's access points has appeared at another RoamAbout switch in the Mobility Domain. • ROAMING AWAY—The RoamAbout switch has been sent a request to transfer the user, who is roaming, to another RoamAbout switch . • STATUS UPDATED—RoamAbout switch is receiving a final update from an access point about the user, who has roamed away. • WEB_AUTHING—User is being authenticated by WebAAA. • WIRED AUTH'ING—User is being authenticated by the 802.1X protocol on a wired authentication port. • KILLING—User's session is being cleared, because of 802.1X authentication failure, entry of a **clear** command, or some other event.
Port/Radio	Number of the port and radio through which the user is accessing this session.
MAC address	MAC address of the session user.
User Name	Name of the authenticated user of this session
IP Address	IP address of the session user.
Vlan Name	Name of the VLAN associated with the session.
Tag	System-wide supported VLAN tag type.
Session Timeout	Assigned session timeout in seconds.
Authentication Method	Extensible Authentication Protocol (EAP) type used to authenticate the session user, and the IP address of the authentication server.
Session statistics as updated from AP	Time the session statistics were last updated from the access point, in seconds since a fixed standard date and time.
Unicast packets in	Total number of unicast packets received from the user by the RoamAbout switch (64-bit counter).
Unicast bytes in	Total number of unicast bytes received from the user by the RoamAbout switch (64-bit counter).
Unicast packets out	Total number of unicast packets sent by the RoamAbout switch to the user (64-bit counter).

Table 18-5 Output for show sessions network session-id (continued)

Output	What It Displays...
Unicast bytes out	Total number of unicast bytes sent by the RoamAbout switch to the user (64-bit counter).
Multicast packets in	Total number of multicast packets received from the user by the RoamAbout switch (64-bit counter).
Multicast bytes in	Total number of multicast bytes received from the user by the RoamAbout switch (64-bit counter).
Number of packets with encryption errors	Total number of decryption failures.
Number of bytes with encryption errors	Total number of bytes with decryption errors.
Last packet data rate	Data transmit rate, in megabits per second (Mbps), of the last packet received by the access point.
Last packet signal strength	Signal strength, in decibels referred to 1 milliwatt (dBm), of the last packet received by the access point.
Last packet data S/N ratio	Signal-to-noise ratio of the last packet received by the access point.

Related Commands

clear sessions network on page 18-3

19

RF Detection Commands

MSS automatically performs RF detection scans on enabled and disabled radios to detect rogue access points. A rogue access point is a BSSID (MAC address associated with an SSID) that does not belong to an Enterasys Networks device and is not a member of the ignore list configured on the seed switch of the Mobility Domain.

MSS can issue countermeasures against rogue devices to prevent clients from being able to use them.

You can configure RF detection parameters on individual RoamAbout switches.

You can configure RF detection parameters only on the seed switch of a Mobility Domain.

This chapter presents RF detection commands alphabetically. Use the following table to locate the commands in this chapter.

For information about...	Refer to page...
clear rfdetect attack-list	19-3
clear rfdetect black-list	19-4
clear rfdetect countermeasures mac	19-5
clear rfdetect ignore	19-6
clear rfdetect ssid-list	19-7
clear rfdetect vendor-list	19-8
set rfdetect attack-list	19-9
set rfdetect attack-list	19-9
set rfdetect black-list	19-10
set rfdetect ignore	19-11
set rfdetect log	19-12
set rfdetect signature	19-13
set rfdetect ssid-list	19-14
set rfdetect vendor-list	19-15
show rfdetect attack-list	19-16
show rfdetect black-list	19-17
show rfdetect clients	19-18
show rfdetect countermeasures	19-21

For information about...	Refer to page...
show rfdetect countermeasures	19-21
show rfdetect countermeasures	19-21
show rfdetect data	19-23
show rfdetect ignore	19-25
show rfdetect mobility-domain	19-26
show rfdetect ssid-list	19-30
show rfdetect vendor-list	19-31
show rfdetect visible	19-32
test rflink	19-35

clear rfdetect attack-list

Removes a MAC address from the attack list.

Syntax

clear rfdetect attack-list *mac-addr*

Parameters

mac-addr	MAC address you want to remove from the attack list.

Defaults

None.

Mode

Enabled.

Example

The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
RBT-8100# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer in attacklist.
```

Related Commands

- set rfdetect attack-list on page 19-9
- show rfdetect attack-list on page 19-16

clear rfdetect black-list

Removes a MAC address from the client black list.

Syntax

clear rfdetect black-list *mac-addr*

Parameters

mac-addr	MAC address you want to remove from the black list.

Defaults

None.

Mode

Enabled.

Example

The following command removes MAC address 11:22:33:44:55:66 from the black list:

```
RBT-8100# clear rfdetect black-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer blacklisted.
```

Related Commands

- set rfdetect black-list on page 19-10
- show rfdetect black-list on page 19-17

clear rfdetect countermeasures mac

Removes a rogue BSSID from the list configured by the **set rfdetect countermeasures mac** command.

Syntax

```
set rfdetect countermeasures mac
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Usage

This command applies only to rogue devices that you explicitly started countermeasures against using the **set rfdetect countermeasures mac** command. This command is valid only on the seed switch of the Mobility Domain, and does not become part of the configuration file when you save the configuration and therefore is not reloaded if the switch is restarted.

After you type the first **set rfdetect countermeasures mac** command, MSS does not issue countermeasures against any devices *except* the ones you specify using this command. To resume normal countermeasures operation, where MSS automatically issues countermeasures against detected rogues, use the **clear rfdetect countermeasures mac all** command.

If the **clear rfdetect countermeasures mac** command removes the last rogue from the list created by **set rfdetect countermeasures mac** commands, RF detection returns to the default handling of countermeasures. Consequently, the rogue you cleared can still be attacked if it is still in the rogue list. To stop countermeasures against a device, add the device to the known addresses list using the **set rfdetect ignore** command.

Example

The following command removes rogue BSSID aa:bb:cc:11:22:33 from the list configured by the **set rfdetect countermeasures mac** command:

```
RBT-8100# clear rfdetect countermeasures mac aa:bb:cc:11:22:33
success:  clear rfdetect countermeasures mac aa:bb:cc:11:22:33
```

Related Commands

- set rfdetect ignore on page 19-11
- set rfdetect ignore on page 19-11
- show rfdetect countermeasures on page 19-21

clear rfdetect ignore

Removes a device from the ignore list for RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax

clear rfdetect ignore *mac-addr*

Parameters

mac-addr	Basic service set identifier (BSSID), which is a MAC address, of the device to remove from the ignore list.

Defaults

None.

Mode

Enabled.

Example

The following command removes BSSID *aa:bb:cc:11:22:33* from the ignore list for RF scans:

```
RBT-8100# clear rfdetect ignore aa:bb:cc:11:22:33
success: aa:bb:cc:11:22:33 is no longer ignored.
```

Related Commands

- set rfdetect ignore on page 19-11
- show rfdetect ignore on page 19-25

clear rfdetect ssid-list

Removes an SSID from the permitted SSID list.

Syntax

clear rfdetect ssid-list *ssid-name*

Parameters

ssid-name	SSID name you want to remove from the permitted SSID list.

Defaults

None.

Mode

Enabled.

Example

The following command clears SSID *mycorp* from the permitted SSID list:

```
RBT-8100# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

Related Commands

- set rfdetect ssid-list on page 19-14
- show rfdetect ssid-list on page 19-30

clear rfdetect vendor-list

Removes an entry from the permitted vendor list.

Syntax

clear rfdetect vendor-list {**client** | **ap** | **all**} *mac-addr* | **all-macs**

Parameters

client | **ap** | **all**	Specifies whether the entry is for an AP brand or a client brand, or both types.
mac-addr | **all-macs**	Organizationally Unique Identifier (OUI) to remove, or all of them.

Defaults

None.

Mode

Enabled.

Example

The following command removes client OUI aa:bb:cc:00:00:00 from the permitted vendor list:

```
RBT-8100# clear rfdetect vendor-list client aa:bb:cc:00:00:00
success: aa:bb:cc:00:00:00 is no longer in client vendor-list.
```

Related Commands

- set rfdetect vendor-list on page 19-15
- show rfdetect vendor-list on page 19-31

set rfdetect attack-list

Adds an entry to the attack list. The attack list specifies the MAC addresses of devices that MSS should issue countermeasures against whenever the devices are detected on the network. The attack list can contain the MAC addresses of APs and clients.

Syntax

set rfdetect attack-list *mac-addr*

Parameters

mac-addr	MAC address you want to attack.

Defaults

The attack list is empty by default.

Mode

Enabled.

Usage

The attack list applies only to the RoamAbout switch on which the list is configured. RoamAbout switches do not share attack lists.

Example

The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
RBT-8100# set rfdetect attack-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now in attacklist.
```

Related Commands

- clear rfdetect attack-list on page 19-3
- show rfdetect attack-list on page 19-16

set rfdetect black-list

Adds an entry to the client black list. The client black list specifies clients that are not allowed on the network. MSS drops all packets from the clients on the black list.

Syntax

set rfdetect black-list *mac-addr*

Parameters

mac-addr	MAC address you want to place on the black list.

Defaults

The client black list is empty by default.

Mode

Enabled.

Usage

In addition to manually configured entries, the list can contain entries added by MSS. MSS can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the RoamAbout switch on which the list is configured. RoamAbout switches do not share client black lists.

Example

The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
RBT-8100# set rfdetect black-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now blacklisted.
```

Related Commands

- set rfdetect black-list on page 19-10
- show rfdetect black-list on page 19-17

set rfdetect ignore

Configures a list of known devices to ignore during an RF scan. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax

set rfdetect ignore *mac-addr*

Parameters

mac-addr	BSSID (MAC address) of the device to ignore.

Defaults

MSS reports all non-Enterasys Networks BSSIDs detected during an RF scan.

Mode

Enabled.

Usage

Use this command to identify third-party APs and other devices you are already aware of and do not want MSS to report following RF scans.

If you try to initiate countermeasures against a device on the ignore list, the ignore list takes precedence and MSS does not issue the countermeasures. Countermeasures apply only to rogue devices.

f you add a device that MSS has classified as a rogue to the permitted vendor list or permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list or permitted SSID list merely indicates that the device is from an allowed manufacturer or is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list

Example

The following command configures MSS to ignore BSSID *aa:bb:cc:11:22:33* during RF scans:

```
RBT-8100# set rfdetect ignore aa:bb:cc:11:22:33
success:  MAC aa:bb:cc:11:22:33 is now ignored.
```

Related Commands

- clear rfdetect ignore on page 19-6
- show rfdetect ignore on page 19-25

set rfdetect log

Disables or reenables generation of log messages when rogues are detected or when they disappear.

Syntax

```
set rfdetect log {enable | disable}
```

Parameters

enable	Enables logging of rogues.
disable	Disables logging of rogues.

Defaults

RF detection logging is enabled by default.

Mode

Enabled.

Usage

This command is valid only on the seed switch of the Mobility Domain.

The log messages for rogues are generated only on the seed and appear only in the seed's log message buffer. Use the **show log buffer** command to display the messages in the seed switch's log message buffer.

Example

The following command enables RF detection logging for the Mobility Domain managed by this seed switch:

```
RBT-8100# set rfdetect log enable
success:  rfdetect logging is enabled.
```

Related Commands

show log buffer on page 23-7

set rfdetect signature

Enables access point signatures. An access point signature is a set of bits in a management frame sent by an access point that identifies that access point to MSS. If someone attempts to spoof management packets from an Enterasys Networks access point, MSS can detect the spoof attempt.

Syntax

```
set rfdetect signature {enable | disable}
```

Parameters

enable	Enables access point signatures.
disable	Disables access point signatures.

Defaults

access point signatures are disabled by default.

Mode

Enabled.

Usage

The command applies only to access points managed by the RoamAbout switch on which you enter the command. To enable signatures on all access points in a Mobility Domain, enter the command on each RoamAbout switch in the Mobility Domain.

Note: You must use the same access point signature setting (enabled or disabled) on all RoamAbout switches in a Mobility Domain.

Example

The following command enables access point signatures on a RoamAbout switch:

```
RBT-8100# set rfdetect signature enable
success:  signature is now enabled.
```

set rfdetect ssid-list

Adds an SSID to the permitted SSID list.The permitted SSID list specifies the SSIDs that are allowed on the network. If MSS detects packets for an SSID that is not on the list, the AP that sent the packets is classified as a rogue. MSS issues countermeasures against the rogue if they are enabled.

Syntax

set rfdetect ssid-list *ssid-name*

Parameters

ssid-name	SSID name you want to add to the permitted SSID list.

Defaults

The permitted SSID list is empty by default and all SSIDs are allowed. However, after you add an entry to the list, MSS allows traffic only for the SSIDs that are on the list.

Mode

Enabled.

Usage

The permitted SSID list applies only to the RoamAbout switch on which the list is configured. RoamAbout switches do not share permitted SSID lists.

Example

The following command adds SSID *mycorp* to the list of permitted SSIDs:

```
RBT-8100# set rfdetect ssid-list mycorp
success:  ssid mycorp is now in ssid-list.
```

Related Commands

- clear rfdetect ssid-list on page 19-7
- show rfdetect ssid-list on page 19-30

set rfdetect vendor-list

Adds an entry to the permitted vendor list. The permitted vendor list specifies the third-party AP or client vendors that are allowed on the network. MSS does not list a device as a rogue or interfering device if the device's OUI is in the permitted vendor list.

Syntax

set rfdetect vendor-list {**client** | **ap**} *mac-addr*

Parameters

client | **ap**	Specifies whether the entry is for an AP brand or a client brand.
mac-addr | **all**	Organizationally Unique Identifier (OUI) to remove.

Defaults

The permitted vendor list is empty by default and all vendors are allowed. However, after you add an entry to the list, MSS allows only the devices whose OUIs are on the list.

Mode

Enabled.

Usage

The permitted vendor list applies only to the RoamAbout switch on which the list is configured. RoamAbout switches do not share permitted vendor lists.

Example

The following command adds an entry for clients whose MAC addresses start with aa:bb:cc:

```
RBT-8100# set rfdetect vendor-list client aa:bb:cc:00:00:00
success:  MAC aa:bb:cc:00:00:00 is now in client vendor-list.
```

The trailing 00:00:00 value is required.

Related Commands

- clear rfdetect vendor-list on page 19-8
- show rfdetect vendor-list on page 19-31

show rfdetect attack-list

Displays information about the MAC addresses in the attack list.

Syntax

show rfdetect attack-list

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following example shows the attack list on RoamAbout switch:

```
RBT-8100# show rfdetect attack-list
Total number of entries: 1
 Attacklist MAC    Port/Radio/Chan   RSSI      SSID
----------------- ----------------- ------ ------------
11:22:33:44:55:66  dap 2/1/11       -53    rogue-ssid
```

Related Commands

- clear rfdetect attack-list on page 19-3
- set rfdetect attack-list on page 19-9

show rfdetect black-list

Displays information abut the clients in the client black list.

Syntax

show rfdetect black-list

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following example shows the client black list on RoamAbout switch:

```
RBT-8100# show rfdetect black-list
Total number of entries: 1
  Blacklist MAC         Type          Port   TTL
----------------- ----------------- ------- ---
11:22:33:44:55:66 configured        -         -
11:23:34:45:56:67 assoc req flood   3        25
```

Related Commands

- clear rfdetect black-list on page 19-4
- set rfdetect black-list on page 19-10

show rfdetect clients

Displays the wireless clients detected by a RoamAbout switch.

Syntax

show rfdetect clients [**mac** *mac-addr*]

Parameters

mac *mac-addr*	Displays detailed information for a specific client.

Defaults

None.

Mode

Enabled.

Examples

The following command shows information about all wireless clients detected by a RoamAbout switch's access points:

```
RBT-8100# show rfdetect clients
Total number of entries: 30
Client MAC        Client       AP MAC          AP    Port/Radio    NoL Type  Last
                  Vendor                     Vendor      /Channel            seen
----------------- ------- ----------------- ------- ------------- --- ----- ----

00:03:7f:bf:16:70 Unknown           Unknown           dap 1/1/6     1 intfr 207
00:04:23:77:e6:e5   Intel           Unknown           dap 1/1/2     1 intfr 155
00:05:5d:79:ce:0f  D-Link           Unknown           dap 1/1/149   1 intfr 87
00:05:5d:7e:96:a7  D-Link           Unknown           dap 1/1/149   1 intfr 117
00:05:5d:7e:96:ce  D-Link           Unknown           dap 1/1/157   1 intfr 162
00:05:5d:84:d1:c5  D-Link           Unknown           dap 1/1/1     1 intfr 52
```

The following command displays more details about a specific client:

```
RBT-8100# show rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys
    Port: dap 1, Radio: 1, Channel: 11, RSSI: -82, Rate: 2, Last Seen (secs ago):
84
    Bssid: 00:0b:0e:01:02:00, Vendor: Enterasys Networks, Type: intfr, Dst:
ff:ff:ff:ff:ff:ff
    Last Rogue Status Check (secs ago): 3
```

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

Table 19-1 and Table 19-2 describe the fields in these displays.

Table 19-1 show rfdetect clients Output

Output	What it displays...
Client MAC	MAC address of the client.
Client Vendor	Company that manufactures or sells the client.
AP MAC	MAC address of the radio with which the rogue client is associated.
AP Vendor	Company that manufactures or sells the AP with which the rogue client is associated.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed access point, the connection number is labeled *dap*. (This stands for *distributed ap*.)
NoL	Number of listeners. This is the number of access point radios that detected the rogue client.
Type	Classification of the rogue device: • rogue—Wireless device that is on the network but is not supposed to be on the network. • intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Last seen	Number of seconds since an access point radio last detected 802.11 packets from the device.

Table 19-2 show rfdetect clients mac Output

Output	What it displays...
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).
Rate	The data rate of the client.
Last Seen	Number of seconds since an access point radio last detected 802.11 packets from the device.
BSSID	MAC address of the SSID with which the rogue client is associated.
Vendor	Company that manufactures or sells the AP with which the rogue client is associated.
Typ	Classification of the rogue device: • rogue—Wireless device that is on the network but is not supposed to be on the network. • intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Dst	MAC addressed to which the last 802.11 packet detected from the client was addressed.

Table 19-2 show rfdetect clients mac Output (continued)

Output	What it displays...
Last Rogue Status Check	Number of seconds since the RoamAbout switch looked on the air for the AP with which the rogue client is associated. The switch looks for the client's AP by sending a packet from the wired side of the network addressed to the client, and watching the air for a wireless packet containing the client's MAC address.

show rfdetect countermeasures

Displays the current status of countermeasures against rogues in the Mobility Domain.

Syntax

show rfdetect countermeasures

Parameters

None.

Defaults

None.

Mode

Enabled.

Usage

This command is valid only on the seed switch of the Mobility Domain.

Examples

The following example displays countermeasures status for the Mobility Domain:

```
RBT-8100# show rfdetect countermeasures
Total number of entries: 190
Rogue MAC         Type  Countermeasures    RBT-IPaddr       Port/Radio
                        Radio Mac                              /Channel
----------------- ----- ------------------ --------------- -------------
00:0b:0e:00:71:c0 intfr  00:0b:0e:44:55:66 10.1.1.23       dap 4/1/6
00:0b:0e:03:00:80 rogue  00:0b:0e:11:22:33 10.1.1.23       dap 2/1/11
```

Table 19-3 describes the fields in this display.

Table 19-3 show rfdetect countermeasures Output

Output	What it displays...
Rogue MAC	BSSID of the rogue.
Type	Classification of the rogue device: • rogue—Wireless device that is on the network but is not supposed to be on the network. • intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Countermeasures Radio MAC	MAC address of the Enterasys Networks radio sending countermeasures against the rogue.
RAS-IPaddr	System IP address of the RoamAbout switch that is managing the access point that is sending or will send countermeasures.

Table 19-3 show rfdetect countermeasures Output (continued)

Output	What it displays...
Rogue MAC	BSSID of the rogue.
Type	Classification of the rogue device: • rogue—Wireless device that is on the network but is not supposed to be on the network. • intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Port/Radio/Channel	Port number, radio number, and channel number of the countermeasures radio. For a Distributed access point, the connection number is labeled *dap*. (This stands for *distributed ap*.)

```
RBT-8100# show rfdetect countermeasures
Total number of entries: 8
    Rogue MAC          Countermeasures    RBT-IPaddr        Port/Radio
                       Radio Mac                                /Channel
    ------------------ ------------------ --------------- -------------
    00:00:00:01:7a:80  00:0b:0e:00:0a:a3    10.8.121.101       5/2/60
    00:0b:0e:08:1a:01        Not Started
    00:0b:0e:01:00:00        Not Started
    00:0b:0e:00:03:80  00:0b:0e:00:0a:6a    10.8.121.102       3/1/1
    00:0b:0e:00:d1:00  00:0b:0e:00:0a:6a    10.8.121.102       3/1/11
    00:0b:0e:00:7a:80  00:0b:0e:00:0a:6b    10.8.121.102       3/2/60
    00:06:25:51:e9:ff        Not Started
    00:0b:0e:01:08:40  00:0b:0e:00:0a:6a    10.8.121.102       3/1/1
```

Related Commands

- set radio-profile countermeasures on page 11-57
- clear rfdetect countermeasures mac on page 19-5
- set rfdetect ignore on page 19-11

show rfdetect data

Displays information about the APs detected by a RoamAbout switch.

Displays all the BSSIDs detected by an individual RoamAbout switch during an RF detection scan. The data includes BSSIDs transmitted by other Enterasys Networks radios as well as by third-party access points.

Syntax

show rfdetect data

Defaults

None.

Mode

Enabled.

Usage

You can enter this command on any RoamAbout switch in the Mobility Domain. The output applies only to the switch on which you enter the command. To display all devices that a specific Enterasys Networks radio has detected, even if the radio is managed by another RoamAbout switch, use the **show rfdetect visible** command.

To display rogue information for the entire Mobility Domain, use the **show rfdetect mobility-domain** command on the seed switch.

Only one MAC address is listed for each Enterasys Networks radio, even if the radio is beaconing multiple SSIDs.

Examples

The following command shows the devices detected by this RoamAbout switch during the most recent RF detection scan:

```
RBT-8100# show rfdetect data
Total number of entries: 197
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor  Type  Port/Radio/Ch Flags  RSSI Age SSID
----------------- ------- ----- ------------- ------ ---- --- -----------------
00:07:50:d5:cc:91   Cisco intfr       3/1/6   i----w  -61   6 r27-cisco1200-2
00:07:50:d5:dc:78   Cisco intfr       3/1/6   i----w  -82   6 r116-cisco1200-2
00:09:b7:7b:8a:54   Cisco intfr       3/1/2   i-----  -57   6
00:0a:5e:4b:4a:c0    3Com intfr       3/1/11  i-----  -57   6 public
00:0a:5e:4b:4a:c2    3Com intfr       3/1/11  i-t1--  -86   6 enterasyswlan
00:0a:5e:4b:4a:c4    3Com intfr       3/1/11  ic----  -85   6 ets-ccmp
00:0a:5e:4b:4a:c6    3Com intfr       3/1/11  i-t---  -85   6 ets-tkip
00:0a:5e:4b:4a:c8    3Com intfr       3/1/11  i----w  -83   6 ets-voip
00:0a:5e:4b:4a:ca    3Com intfr       3/1/11  i-----  -85   6 ets-webaaa
...
```

Table 19-4 describes the fields in this display.

Table 19-4 show rfdetect data Output

Output	What it displays...
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: • rogue—Wireless device that is not supposed to be on the network. The device has an entry in a RoamAbout switch's FDB and is therefore on the network. • intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a RoamAbout switch's FDB and is not actually on the network, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed access point, the connection number is labeled *dap*. (This stands for *distributed ap*.)
Flags	Classification and encryption information for the rogue: • The i, a, or u flag indicates the classification. • The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).
Age	Number of seconds since an access point radio last detected 802.11 packets from the device.
SSID	SSID used by the detected device.

```
RBT-8100# show rfdetect data
Total number of entries: 7
          BSSID        Port/Rad   Chan   RSSI Age SSID
    -----------------  --------  ------  ---- --- --------
    00:06:25:09:39:4a     5/1         3  0     15 rack29-hostap
    00:06:25:51:e9:ff     4/1        10  -85   15 Arrow
    00:06:25:51:e9:ff     5/1        10  -84   15 Arrow
    00:0b:0e:00:00:00     4/1         1  -78   15 gary-eng
    00:0b:0e:00:02:00     4/1        11  -76   15 public
    00:0b:0e:00:02:00     5/1        11  -74   15 public
    00:0b:0e:00:02:01     4/1        56  -68   15 public
```

Related Commands

- show rfdetect mobility-domain on page 19-26
- show rfdetect visible on page 19-32

show rfdetect ignore

Displays the BSSIDs of third-party devices that MSS ignores during RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax

show rfdetect ignore

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following example displays the list of ignored devices:

```
RBT-8100# show rfdetect ignore
Total number of entries: 2
   Ignore MAC
-----------------
aa:bb:cc:11:22:33
aa:bb:cc:44:55:66
```

Related Commands

- clear rfdetect ignore on page 19-6
- set rfdetect ignore on page 19-11

show rfdetect mobility-domain

Displays the rogues detected by all RoamAbout switches in the Mobility Domain during RF detection scans.

Syntax

show rfdetect mobility-domain [**ssid** *ssid-name* | **bssid** *mac-addr*]

Parameters

ssid *ssid-name*	Displays rogues that are using the specified SSID.
bssid *mac-addr*	Displays rogues that are using the specified BSSID.

Defaults

None.

Mode

Enabled.

Usage

This command is valid only on the seed switch of the Mobility Domain. To display rogue information for an individual switch, use the **show rfdetect data** command on that switch.

Only rogues are listed. To display all devices detected, including Enterasys Networks radios, use the **show rfdetect data** command.

Examples

The following command displays summary information for all SSIDs and BSSIDs detected in the Mobility Domain:

```
RBT-8100# show rfdetect mobility-domain
Total number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor       Type  Flags  SSID
----------------- ------------ ----- ------ --------------------------------
00:07:50:d5:cc:91        Cisco intfr i----w r27-cisco1200-2
00:07:50:d5:dc:78        Cisco intfr i----w r116-cisco1200-2
00:09:b7:7b:8a:54        Cisco intfr i-----
00:0a:5e:4b:4a:c0         3Com intfr i----- public
00:0a:5e:4b:4a:c2         3Com intfr i----w enterasyswlan
00:0a:5e:4b:4a:c4         3Com intfr ic---- ets-ccmp
00:0a:5e:4b:4a:c6         3Com intfr i----w ets-tkip
00:0a:5e:4b:4a:c8         3Com intfr i----w ets-voip
00:0a:5e:4b:4a:ca         3Com intfr i----- ets-webaaa
...
```

The lines in this display are compiled from data from multiple listeners (access point radios). If an item has the value *unresolved*, not all listeners agree on the value for that item. Generally, an unresolved state occurs only when an access point or a Mobility Domain is still coming up, and lasts only briefly.

The following command displays detailed information for rogues using SSID *ets-webaaa*.

```
RBT-8100# show rfdetect mobility-domain ssid ets-webaaa
BSSID: 00:0a:5e:4b:4a:ca Vendor: 3Com SSID: ets-webaaa
Type: intfr Adhoc: no Crypto-types: clear

  RBT-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/11 Mac: 00:0b:0e:00:0a:6a
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -85 SSID: ets-webaaa

BSSID: 00:0b:0e:00:7a:8a Vendor: enterasys SSID: ets-webaaa
Type: intfr Adhoc: no Crypto-types: clear

  RBT-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/1 Mac: 00:0b:0e:00:0a:6a
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -75 SSID: ets-webaaa

  RBT-IPaddress: 10.3.8.103 Port/Radio/Ch: dap 1/1/1 Mac: 00:0b:0e:76:56:82
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -76 SSID: ets-webaaa
```

Two types of information are shown. The lines that are not indented show the BSSID, vendor, and information about the SSID. The indented lines that follow this information indicate the listeners (access point radios) that detected the SSID. Each set of indented lines is for a separate access point listener.

In this example, two BSSIDs are mapped to the SSID. Separate sets of information are shown for each of the BSSIDs, and information about the listeners for each BSSID is shown.

The following command displays detailed information for a BSSID.

```
RBT-8100# show rfdetect mobility-domain bssid 00:0b:0e:00:04:d1
BSSID: 00:0b:0e:00:04:d1 Vendor: Cisco SSID: notmycorp
Type: rogue Adhoc: no Crypto-types: clear

  RBT-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/2/56 Mac: 00:0b:0e:00:0a:6b
Device-type: rogue Adhoc: no Crypto-types: clear
RSSI: -72 SSID: notmycorp

  RBT-IPaddress: 10.3.8.103 Port/Radio/Ch: dap 1/1/157 Mac: 00:0b:0e:76:56:82
  Device-type: rogue Adhoc: no Crypto-types: clear
  RSSI: -72 SSID: notmycorp
```

Table 19-5 and Table 19-6 describe the fields in these displays.

Table 19-5 show rfdetect mobility-domain Output

Output	What it displays...
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: • rogue—Wireless device that is not supposed to be on the network. The device has an entry in a RoamAbout switch's FDB and is therefore on the network. • intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a RoamAbout switch's FDB and is not actually on the network, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Flags	Classification and encryption information for the rogue: • The i, a, or u flag indicates the classification. • The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

Table 19-6 show rfdetect mobility-domain ssid or bssid Output

Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
SSID	SSID used by the detected device.
Type	Classification of the rogue device: • rogue—Wireless device that is on the network but is not supposed to be on the network. • intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Adhoc	Indicates whether the rogue is an infrastructure rogue (is using an AP) or is operating in ad-hoc mode.
Crypto-Types	Encryption type: • clear (no encryption) • ccmp • tkip • wep104 (WPA 104-bit WEP) • wep40 (WPA 40-bit WEP) • wep (non-WPA WEP)
RAS-IPaddress	System IP address of the RoamAbout switch that detected the rogue.

Table 19-6 show rfdetect mobility-domain ssid or bssid Output (continued)

Field	Description
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed access point, the connection number is labeled *dap*. (This stands for *distributed ap*.)
Mac	MAC address of the radio that detected the rogue.
Device-type	Device type detected by the access point radio.
Adhoc	Ad-hoc status (yes or no) detected by the access point radio.
Crypto-Types	Encryption type detected by the access point radio.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).
SSID	SSID mapped to the BSSID.

```
RBT-8100# show rfdetect mobility-domain
Total number of entries: 3
BSSID                  RBT-IPaddr       Port/Radio    RSSI SSID
   > Radio Mac                              /Channel
---------------------- --------------- ------------- ---- -----------
00:00:00:01:7a:80
   > 00:0b:0e:00:0a:a3    10.8.121.101       5/2/60   -34 enterasyswla
   > 00:0b:0e:00:04:c8    10.8.121.101       4/2/60   -46 enterasyswla
   > 00:0b:0e:00:0a:6b    10.8.121.102       3/2/60   -32 enterasyswla
00:00:00:01:d1:41
   > 00:0b:0e:00:04:c8    10.8.121.101       4/2/36   -37 enterasyswla
   > 00:0b:0e:00:0a:a3    10.8.121.101       5/2/36   -33 enterasyswla
00:00:00:01:d9:41
   > 00:0b:0e:00:0a:a3    10.8.121.101       5/2/52   -66 public
   > 00:0b:0e:00:0a:6b    10.8.121.102       3/2/52   -54 public
```

Related Commands

- show rfdetect data on page 19-23
- show rfdetect visible on page 19-32

show rfdetect ssid-list

Displays the entries in the permitted SSID list.

Syntax

show rfdetect ssid-list

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following example shows the permitted SSID list on RoamAbout switch:

```
RBT-8100# show rfdetect ssid-list
Total number of entries: 3
       SSID
-----------------
           mycorp
        corporate
            guest
```

Related Commands

- clear rfdetect ssid-list on page 19-7
- set rfdetect ssid-list on page 19-14

show rfdetect vendor-list

Displays the entries in the permitted vendor list.

Syntax

show rfdetect vendor-list

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

The following example shows the permitted vendor list on RoamAbout switch:

```
RBT-8100# show rfdetect vendor-list
Total number of entries: 1
       OUI         Type
----------------- ------
aa:bb:cc:00:00:00 client
11:22:33:00:00:00 ap
```

Related Commands

- clear rfdetect vendor-list on page 19-8
- set rfdetect vendor-list on page 19-15

show rfdetect visible

Displays the BSSIDs discovered by a specific Enterasys Networks radio. The data includes BSSIDs transmitted by other Enterasys Networks radios as well as by third-party access points.

Syntax

show rfdetect visible *mac-addr*

show rfdetect visible dap *dap-num* [**radio** {**1** | **2**}]

Parameters

mac-addr	Base MAC address of the Enterasys Networks radio. **Note:** To display the base MAC address of an Enterasys Networks radio, use the **show {ap | dap} status** command.
dap-num	Number of a Distributed access point for which to display neighboring BSSIDs.
radio 1	Shows neighbor information for radio 1.
radio 2	Shows neighbor information for radio 2. (This option does not apply to single-radio models.)

Defaults

None.

Mode

Enabled.

Usage

If an Enterasys Networks radio is supporting more than one SSID, each of the corresponding BSSIDs is listed separately.

To display rogue information for the entire Mobility Domain, use the **show rfdetect mobility-domain** command on the seed switch.

Example

To following command displays information about the rogues detected by radio 1 on access point port 3:

```
RBT-8100# show rfdetect visible ap 3 radio 1
Total number of entries: 104
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
Transmit MAC      Vendor  Type  Ch  RSSI Flags  SSID
----------------- ------- ----- --- ---- ------ --------------------------------
00:07:50:d5:cc:91   Cisco intfr   6  -60 i----w r27-cisco1200-2
00:07:50:d5:dc:78   Cisco intfr   6  -82 i----w r116-cisco1200-2
00:09:b7:7b:8a:54   Cisco intfr   2  -54 i-----
00:0a:5e:4b:4a:c0    3Com intfr  11  -57 i----- public
00:0a:5e:4b:4a:c2    3Com intfr  11  -86 i-t1-- enterasyswlan
```

```
00:0a:5e:4b:4a:c4    3Com intfr  11  -85 ic---- ets-ccmp
00:0a:5e:4b:4a:c6    3Com intfr  11  -85 i-t--- ets-tkip
00:0a:5e:4b:4a:c8    3Com intfr  11  -83 i----w ets-voip
00:0a:5e:4b:4a:ca    3Com intfr  11  -85 i----- ets-webaaa
...
```

Table 19-7 describes the fields in this display.

Table 19-7 show rfdetect visible Output

Output	What it displays...
Transmit MAC	MAC address the rogue device that sent the 802.11 packet detected by the access point radio.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: • rogue—Wireless device that is on the network but is not supposed to be on the network. • intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with access point radios. • known—Device that is a legitimate member of the network.
Ch	Channel number on which the radio detected the rogue.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm).
Flags	Classification and encryption information for the rogue: • The i, a, or u flag indicates the classification. • The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

Examples

The following command displays the devices detected by Enterasys Networks radio 00:0b:0e:00:0a:6a:

```
RBT-8100# show rfdetect visible 00:0b:0e:00:0a:6a
Total number of entries: 4
      Transmit MAC       Chan      RSS
    -----------------  --------  -------
     00:0b:0e:00:02:01     56     -74
     00:0b:0e:00:03:41     36     -44
     00:0b:0e:00:0b:01     52     -79
     00:0b:0e:ff:00:01     36     -84
```

The following command displays the devices detected by Enterasys Networks radio 1 on the access point connected to RoamAbout port 3:

```
RBT-8100# show rfdetect visible ap 3 radio 1
Total number of entries: 3
      Transmit MAC       Chan      RSS
    -----------------  --------  -------
     00:06:25:51:e9:ff     10     -77
     00:0b:0e:00:03:80      1     -79
     00:0b:0e:00:a6:00      1     -71
```

Related Commands

- show rfdetect data on page 19-23
- show rfdetect mobility-domain on page 19-26

test rflink

Provides information about the RF link between the RoamAbout Switch and the client based on sending test packets to the client.

Syntax

test rflink {**mac** *mac-addr* | **session-id** *session-id*}

Parameters

mac-addr	Tests the RF link between the RoamAbout Switch and the client with the specified MAC address.
session-id	Tests the RF link between the RoamAbout Switch and the client with the specified local session ID.

Defaults

None.

Mode

Enabled.

Usage

Use this command to send test packets to a specified client. The output of the command indicates the number of test packets received and acknowledged by the client, as well as the client's signal strength and signal-to-noise ratio.

Example

The following command tests the RF link between the RoamAbout Switch and the client with MAC address 00:0e:9b:bf:ad:13:

```
RBT-8100# test rflink mac 00:0e:9b:bf:ad:13
RF-Link Test to 00:0e:9b:bf:ad:13 :
Session-Id: 2
Packets Sent  Packets Rcvd  RSSI     SNR    RTT (micro-secs)
------------  ------------  -------  -----  ----------------
          20            20      -68     26               976
```

Table 19-8 describes the fields in this display.

Table 19-8 test rflink Output

Field	Description
Packets Sent	The number of test packets sent from the RoamAbout Switch to the client.
Packets Rcvd	The number of test packets acknowledged by the client.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal from the client, in decibels referred to 1 milliwatt (dBm).

Table 19-8 test rflink Output (continued)

Field	Description
SNR	Signal-to-noise ratio (SNR), in decibels (dB), of the data received from the client.
RTT (micro-secs)	The round-trip time, in microseconds, for the client response to the test packets.

Related Commands

- show rfdetect data on page 19-23
- show rfdetect visible on page 19-32

20

File Management Commands

Use file management commands to manage system files and to display software and boot information. This chapter presents file management commands alphabetically.

Use the following table to locate commands in this chapter.

For information about...	Refer to page...
backup	20-2
clear boot config	20-4
copy	20-5
delete	20-7
dir	20-8
install soda agent	20-10
load config	20-11
md5	20-13
mkdir	20-14
reset system	20-16
restore	20-17
rmdir	20-19
save config	20-20
set boot configuration-file	20-21
set boot partition	20-23
show boot	20-24
show config	20-26
show version	20-28
uninstall soda agent	20-30

backup

Creates an archive of RoamAbout system files and optionally, user file, in Unix *tape archive* (*tar*) format.

Syntax

backup system [**tftp:/***ip-addr***/**]*filename* [**all** | **critical**]

Parameters

[**tftp:/***ip-addr***/**]*filename*	Name of the archive file to create. You can store the file locally in the switch's nonvolatile storage or on a TFTP server.
all	Backs up system files and all the files in the user files area. The user files area contains the set of files listed in the *file* section of **dir** command output.
critical	Backs up system files only, including the configuration file used when booting, and certificate files. The size of an archive created by this option is generally 1MB or less.

Defaults

The default is **all**.

Mode

Enabled.

Usage

You can create an archive located on a TFTP server or in the switch's nonvolatile storage. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the switch.

Use the **critical** option if you want to back up or restore only the system-critical files required to operate and communicate with the switch. Use the **all** option if you also want to back up or restore WebAAA pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

The maximum supported file size is 32 MB. If the file size of the tarball is too large, delete unnecessary files (such as unneeded copies of system image files) and try again, or use the **critical** option instead of the **all** option.

Neither option archives image files or any other files listed in the *Boot* section of **dir** command output. The **all** option archives image files only if they are present in the user files area.

Archive files created by the **all** option are larger than files created by the **critical** option. The file size depends on the files in the user area, and the file can be quite large if the user area contains image files.

The **backup** command places the boot configuration file into the archive. (The boot configuration file is the *Configured boot configuration* in the **show boot** command's output.) If the running configuration contains changes that have not been saved, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration that is currently running on the switch, use the **save config** command to save the running configuration to the boot configuration file, before using the **backup** command.

Example

The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP address, so the archive is not stored locally on the switch.

```
RBT-8100# backup system tftp:/10.10.20.9/sysa_bak critical
success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
```

Related Commands

- dir on page 20-8
- restore on page 20-17

clear boot config

Resets to the factory default the configuration that MSS loads during a reboot.

Syntax

clear boot config

Defaults

None.

Mode

Enabled.

Example

The following commands back up the configuration file on a RoamAbout switch, reset the switch to its factory default configuration, and reboot the switch:

```
RBT-8100# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
RBT-8100# clear boot config
success: Reset boot config to factory defaults.
RBT-8100# reset system force
...... rebooting ......
```

Related Commands

- reset system on page 20-16
- show config on page 20-26

copy

Performs the following copy operations:

- Copies a file from a TFTP server to nonvolatile storage.
- Copies a file from nonvolatile storage or temporary storage to a TFTP server.
- Copies a file from one area in nonvolatile storage to another.
- Copies a file to a new filename in nonvolatile storage.

Syntax

copy *source-url destination-url*

Parameters

source-url	Name and location of the file to copy. The uniform resource locator (URL) can be one of the following: [*subdirname*/]*filename* • **file:**[*subdirname*/]*filename* • **tftp:**//*ip-addr*/[*subdirname*/]*filename* • **tmp:***filename* For the filename, specify between 1 and 128 alphanumeric characters, with no spaces. Enter the IP address in dotted decimal notation. The *subdirname*/ option specifies a subdirectory.
destination-url	Name of the copy and the location where to place the copy. The URL can be one of the following: [*subdirname*/]*filename* • **file:**[*subdirname*/]*filename* • **tftp:**//*ip-addr*/[*subdirname*/]*filename* If you are copying a system image file into nonvolatile storage, the filename must include the boot partition name. You can specify one of the following: • **boot0:**/*filename* • **boot1:**/*filename*

Defaults

None.

Mode

Enabled.

Usage

The *filename* and **file:***filename* URLs are equivalent. You can use either URL to refer to a file in a RoamAbout switch's nonvolatile memory. The **tftp://***ip-addr*/*filename* URL refers to a file on a TFTP server. If DNS is configured on the RoamAbout switch, you can specify a TFTP server's hostname as an alternative to specifying the IP address.

The **tmp:***filename* URL specifies a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage. Temporary storage is reserved for use by MSS.

If you are copying a system image file into nonvolatile storage, the filename must be preceded by the boot partition name, which can be **boot0** or **boot1**. Enter the filename as **boot0:/***filename* or **boot1:/***filename*. You must specify the boot partition that *was not* used to load the currently running image.

The maximum supported file size for TFTP is 32 MB.

Examples

The following command copies a file called *floorrbt* from nonvolatile storage to a TFTP server:

```
RBT-8100# copy floorrbt tftp://10.1.1.1/floorrbt
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The following command copies a file called *closetrbt* from a TFTP server to nonvolatile storage:

```
RBT-8100# copy tftp://10.1.1.1/closetrbt closetrbt
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

The following command copies system image *RBT020101.020* from a TFTP server to boot partition 1 in nonvolatile storage:

```
RBT-8100# copy tftp://10.1.1.107/RBT020101.020 boot1:RBT020101.020
.....................................................................................
.............................success: received 9163214 bytes in 105.939 seconds [
86495 bytes/sec]
```

The following commands rename *test-config* to *new-config* by copying it from one name to the other in the same location, then deleting *test-config*:

```
RBT-8100# copy test-config new-config
RBT-8100# delete test-config
success: file deleted.
```

The following command copies file *corpa-login.html* from a TFTP server into subdirectory *corpa* in a RoamAbout switch's nonvolatile storage:

```
RBT-8100# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

Related Commands

- delete on page 20-7
- dir on page 20-8

delete

Deletes a file.

Caution: MSS does not prompt you to verify whether you want to delete a file. When you press Enter after typing a **delete** command, MSS immediately deletes the specified file.

Note: MSS does not allow you to delete the currently running software image file or the running configuration.

Syntax

delete *url*

Parameters

url	Filename. Specify between 1 and 128 alphanumeric characters, with no spaces. If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **subdir_a/file_a**.

Defaults

None.

Mode

Enabled.

Usage

You might want to copy the file to a TFTP server as a backup before deleting the file.

Example

The following commands copy file *testconfig* to a TFTP server and delete the file from nonvolatile storage:

```
RBT-8100# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
RBT-8100# delete testconfig
success: file deleted.
```

Example

The following command deletes file *dang_doc* from subdirectory *dang*:

```
RBT-8100# delete dang/dang_doc
success: file deleted.
```

Related Commands

- copy on page 20-5
- dir on page 20-8

dir

Displays a list of the files in nonvolatile storage and temporary files.

Syntax

dir [*subdirname*]

Parameters

subdirname	Subdirectory name. If you specify a subdirectory name, the command lists the files in that subdirectory. Otherwise, the command lists the files in the root directory and also lists the subdirectories.

Defaults

None.

Mode

Enabled.

Example

The following command displays the files in the root directory:

```
RBT-8100# dir
================================================================================
file:
Filename                                          Size           Created
file:configuration                                 17 KB      May 21 2004, 18:20:53
file:configuration.txt                            379 bytes   May 09 2004, 18:55:17
file:dangcfg                                       13 KB      May 16 2004, 18:30:44
dangdir/                                        512 bytes   May 16 2004, 17:23:44
old/                                            512 bytes   Sep 23 2003, 21:58:48
Total:          32 Kbytes used, 207824 Kbytes free
================================================================================
Boot:
Filename                                          Size           Created
*boot0:bload                                      746 KB      May 09 2004, 19:02:16
*boot0:rbt030000.020                             8182 KB      May 09 2004, 18:58:16
boot1:rbt030000.020                              8197 KB      May 21 2004, 18:01:02
Boot0: Total:        8928 Kbytes used, 3312 Kbytes free
Boot1: Total:        8197 Kbytes used, 4060 Kbytes free
================================================================================
temporary files:
Filename                                          Size           Created
Total:         0 bytes used, 93537 Kbytes free
Total:  15 Kbytes used, 90941 Kbytes free
```

The following command displays the files in the *old* subdirectory:

```
RBT-8100# dir old
================================================================================
```

```
file:
Filename                                          Size           Created
file:configuration.txt                         3541 bytes    Sep 22 2003, 22:55:44
file:configuration.xml                           24 KB       Sep 22 2003, 22:55:44
Total:          27 Kbytes used, 207824 Kbytes free
```

Table 20-1 describes the fields in the **dir** output.

Table 20-1 Output for dir

Output	What It Displays...
Filename	Filename or subdirectory name. For files, the directory name is shown in front of the filename (for example, file:configuration). The *file:* directory is the root directory. For subdirectories, a forward slash is shown at the end of the subdirectory name (for example, old/). In the boot partitions list (Boot:), an asterisk (*) indicates the boot partition from which the currently running image was loaded and the image filename.
Size	Size in Kbytes or bytes.
Created	System time and date when the file was created or copied onto the switch.
Total	Number of kilobytes in use to store files and the number that are still free.

Related Commands

- copy on page 20-5
- delete on page 20-7

install soda agent

Installs Sygate On-Demand (SODA) agent files in a directory on the RoamAbout Switch.

Syntax

install soda agent *agent-file* **agent-directory** *directory*

Parameters

agent-file	Name of a .zip file on the RoamAbout Switch containing SODA agent files.
directory	Directory on the RoamAbout Switch where SODA agent files are to be installed. The command automatically creates this directory.

Defaults

None.

Mode

Enabled.

Usage

Use this command to install a .zip file containing SODA agent files into a directory on the RoamAbout Switch. Prior to installing the SODA agent files, you must have already copied the .zip file to the RoamAbout Switch. This command creates the specified directory, unzips the file and places the contents into the directory. If the specified directory has the same name as an SSID, then that SSID uses the SODA agent files in the directory if SODA functionality is enabled for the service profile that manages the SSID.

Example

The following command installs the contents of the file *soda.ZIP* into a directory called *sp1*.

```
RBT-8100# install soda agent soda.ZIP agent-directory sp1
This command may take up to 20 seconds...
RBT-8100#
```

Related Commands

- uninstall soda agent on page 20-30
- set service-profile soda mode on page 11-110

load config

Caution: This command completely removes the running configuration and replaces it with the configuration contained in the file. Enterasys Networks recommends that you save a copy of the current running configuration to a backup configuration file before loading a new configuration.

Loads configuration commands from a file and replaces the RoamAbout switch's running configuration with the commands in the loaded file.

Syntax

load config [*url*]

Parameters

url	Filename. Specify between 1 and 128 alphanumeric characters, with no spaces. If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults

The default file location is nonvolatile storage.

Note: The current version supports loading a configuration file only from the switch's nonvolatile storage. You cannot load a configuration file directly from a TFTP server.

If you do not specify a filename, MSS uses the same configuration filename that was used for the previous configuration load. For example, if the RoamAbout switch used *configuration* for the most recent configuration load, MSS uses *configuration* again unless you specify a different filename. To display the filename of the configuration file MSS loaded during the last reboot, use the **show boot** command.

Mode

Enabled.

Usage

This command completely replaces the running configuration with the configuration in the file.

Examples

The following command reloads the configuration from the most recently loaded configuration file:

```
RBT-8100# load config
Reloading configuration may result in lost of connectivity, do you wish to
continue? (y/n) [n]y
success: Configuration reloaded
```

The following command loads configuration file *testconfig1*:

```
RBT-8100# load config testconfig1
Reloading configuration may result in lost of connectivity, do you wish to
continue? (y/n) [n]y
success: Configuration reloaded
```

Related Commands

- save config on page 20-20
- show boot on page 20-24
- show config on page 20-26

md5

Calculates the MD5 checksum for a file in the switch's nonvolatile storage.

Syntax

md5 [**boot0:** | **boot1:**]*filename*

Parameters

boot0: | **boot1:**	Boot partition into which you copied the file.
filename	Name of the file.

Defaults

None.

Mode

Enabled.

Example

You must include the boot partition name in front of the filename. If you specify only the filename, the CLI displays a message stating that the file does not exist.

The following command calculates the checksum for image file RBT040003.020 in boot partition 0:

```
RBT-8100# md5 boot0:RBT040003.020
MD5 (boot0:RBT040003.020) = b9cf7f527f74608e50c70e8fb896392a
```

mkdir

Creates a new subdirectory in nonvolatile storage.

Syntax

mkdir [*subdirname*]

Parameters

subdirname	Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults

None.

Mode

Enabled.

Example

The following commands create a subdirectory called *corp2* and display the root directory to verify the result:

```
RBT-8100# mkdir corp2
success: change accepted.
RBT-8100# dir
================================================================================
file:
Filename                                        Size           Created
file:configuration                               17 KB      May 21 2004, 18:20:53
file:configuration.txt                          379 bytes   May 09 2004, 18:55:17
corp2/                                       512 bytes   May 21 2004, 19:22:09
corp_a/                                      512 bytes   May 21 2004, 19:15:48
file:dangcfg                                     13 KB      May 16 2004, 18:30:44
dangdir/                                     512 bytes   May 16 2004, 17:23:44
old/                                         512 bytes   Sep 23 2003, 21:58:48
Total:          33 Kbytes used, 207822 Kbytes free
================================================================================
Boot:
Filename                                        Size           Created
*boot0:bload                                    746 KB      May 09 2004, 19:02:16
*boot0:rbt030000.020                           8182 KB      May 09 2004, 18:58:16
boot1:rbt030000.020                            8197 KB      May 21 2004, 18:01:02
Boot0: Total:        8928 Kbytes used, 3312 Kbytes free
Boot1: Total:        8197 Kbytes used, 4060 Kbytes free
================================================================================
temporary files:
Filename                                        Size           Created
Total:         0 bytes used, 93537 Kbytes free
```

Related Commands

- dir on page 20-8
- rmdir on page 20-19

reset system

Restarts a RoamAbout switch and reboots the software.

Syntax

reset system [**force**]

Parameters

force	Immediately restarts the system and reboots, without comparing the running configuration to the configuration file.

Defaults

None.

Mode

Enabled.

Usage

If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the running configuration and configuration file do not match, MSS does not restart the RoamAbout switch but instead displays a message advising you to either save the configuration changes or use the **force** option.

Example

The following command restarts a RoamAbout switch that does not have any unsaved configuration changes:

```
RBT-8100# reset system
This will reset the entire system. Are you sure (y/n)y
```

The following commands attempt to restart a RoamAbout switch with a running configuration that has unsaved changes, and then force the switch to restart:

```
RBT-8100# reset system
error: Cannot reset, due to unsaved configuration changes. Use "reset system
force" to override.
RBT-8100# reset system force
...... rebooting ......
```

Related Commands

- save config on page 20-20
- show boot on page 20-24
- show version on page 20-28

restore

Unzips a system archive created by the **backup** command and copies the files from the archive onto the switch.

Syntax

restore system [**tftp:/***ip-addr***/**]*filename* [**all** | **critical**] [**force**]

Parameters

[**tftp:/***ip-addr***/**]*filename*	Name of the archive file to load. The archive can be located in the switch's nonvolatile storage or on a TFTP server.
all	Restores system files ***and*** the user files from the archive.
critical	Restores system files only, including the configuration file used when booting, and certificate files.
force	Replaces files on the switch with those in the archive, even if the switch is not the same as the one from which the archive was created. **Note:** Do not use this option unless advised to do so by Enterasys Networks TAC. If you restore one switch's system files onto another switch, you must generate new key pairs and certificates on the switch.

Defaults

The default is **critical**.

Mode

Enabled.

Usage

If a file in the archive has a counterpart on the switch, the archive version of the file replaces the file on the switch. The **restore** command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.

Note: If the archive's files cannot fit on the switch, the restore operation fails. Enterasys Networks recommends deleting unneeded image files before creating or restoring an archive.

The **backup** command stores the MAC address of the switch in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the switch where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack one switch's archive onto another switch.

Caution: Do not use the **force** option unless you are certain you want to replace the switch's files with files from another switch. If you restore one switch's system files onto another switch, you must generate new key pairs and certificates on the switch.

If the configuration running on the switch is different from the one in the archive or you renamed the configuration file, and you want to retain changes that were made after the archive was created, see the "Managing System Files" chapter of the *RoamAbout Mobility System Software Configuration Guide*

Example

The following command restores system-critical files on a switch, from archive *sysa_bak*:

```
RBT-8100# restore system tftp:/10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386 bytes/sec]

success: restore complete.
```

Related Commands

backup on page 20-2

rmdir

Removes a subdirectory from nonvolatile storage.

Syntax

rmdir [*subdirname*]

Parameters

subdirname	Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults

None.

Mode

Enabled.

Usage

MSS does not allow the subdirectory to be removed unless it is empty. Delete all files from the subdirectory before attempting to remove it.

Example

The following example removes subdirectory *corp2*:

```
RBT-8100# rmdir corp2
success: change accepted.
```

Related Commands

- dir on page 20-8
- md5 on page 20-13

save config

Saves the running configuration to a configuration file.

Syntax

save config [*filename*]

Parameters

filename	Name of the configuration file. Specify between 1 and 128 alphanumeric characters, with no spaces. To save the file in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults

By default, MSS saves the running configuration as the configuration filename used during the last reboot.

Mode

Enabled.

Usage

If you do not specify a filename, MSS replaces the configuration file loaded during the most recent reboot. To display the filename of the configuration file MSS loaded during the most recent reboot, use the **show boot** command.

The command completely replaces the specified configuration file with the running configuration.

Example

The following command saves the running configuration to the configuration file loaded during the most recent reboot. In this example, the filename used during the most recent reboot is *configuration*.

```
RBT-8100# save config
Configuration saved to configuration.
```

The following command saves the running configuration to a file named *testconfig1*:

```
RBT-8100# save config testconfig1
Configuration saved to testconfig1.
```

Related Commands

- load config on page 20-11
- show boot on page 20-24
- show config on page 20-26

set boot configuration-file

Changes the configuration file to load after rebooting.

Syntax

set boot configuration-file *filename*

Parameters

filename	Filename. Specify between 1 and 128 alphanumeric characters, with no spaces. To load the file from a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults

The default configuration filename is *configuration*.

Mode

Enabled.

Usage

The file must be located in the switch's nonvolatile storage.

Example

The following command sets the boot configuration file to *testconfig1*:

```
RBT-8100# set boot configuration-file testconfig1
success: boot config set.
```

set boot image

Changes the software image to load after rebooting a RoamAbout switch running MSS Version 1.0.

Note: This command applies only when upgrading from MSS Version 1.0 to 1.1. The command is deprecated in 1.1.

Syntax

set boot image *filename*

Parameters

filename	Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

Defaults

None.

Mode

Enabled.

Example

The following command sets the boot image to *1_0_upgrade_RBT010101.020*:

```
RBT-8100# set boot image 1_0_upgrade_RBT010101.020
success: Setting image. Check "show boot" for status
```

Related Commands

- set boot configuration-file on page 20-21
- show boot on page 20-24

set boot partition

Specifies the boot partition in which to look for the system image file following the next system reset, software reload, or power cycle.

Syntax

```
set boot partition {boot0 | boot1}
```

Parameters

boot0	Boot partition 0.
boot1	Boot partition 1.

Defaults

By default, a RoamAbout switch uses the same boot partition for the next software reload that was used to boot the currently running image.

Mode

Enabled.

Usage

To determine the boot partition that was used to load the currently running software image, use the **dir** command.

Example

The following command sets the boot partition for the next software reload to partition 1:

```
RBT-8100# set boot partition boot1
success: Boot partition set to boot1.
```

Related Commands

- copy on page 20-5
- dir on page 20-8
- reset system on page 20-16

show boot

Displays the system image and configuration filenames used after the last reboot and configured for use after the next reboot.

Syntax

```
show boot
```

Parameters

None.

Defaults

None.

Mode

Access.

Example

The following command shows the boot information for a RoamAbout switch:

```
RBT-8100# show boot
Configured boot image:           boot0:RBT020003.020
Configured boot configuration:   file:newconfig
Booted version:                  2.0.3
Booted image:                    boot1:RBT020101.020
Booted configuration:            file:configuration
Product model:                   RBT-8100
```

Table 20-2 describes the fields in the output.

Table 20-2 Output for show boot

Output	What It Displays...
Configured boot image	Boot partition and image filename MSS will use to boot next time the software is rebooted.
Configured boot configuration	Configuration filename MSS will use to boot next time the software is rebooted.
Booted version	Software version the switch is running.
Booted image	Boot partition and image filename MSS used the last time the software was rebooted. MSS is running this software image.
Booted configuration	Configuration filename MSS used to load the configuration the last time the software was rebooted.

Related Commands

- clear boot config on page 20-4
- reset system on page 20-16
- set boot configuration-file on page 20-21
- show version on page 20-28

show config

Displays the configuration running on the RoamAbout switch.

Syntax

```
show config [area area] [all]
```

Parameters

area *area*	Configuration area. You can specify one of the following: • **aaa** • **acls** • **ap** • **arp** • **eapol** • **httpd** • **ip** • **ip-config** • **12acl** • **log** • **mobility-domain** • **network-domain** • **ntp** • **portconfig** • **port-group** • **qos** • **radio-profile** • **service-profile** • **sm** • **snmp** • **snoop** • **spantree** • **system** • **trace** • **vlan** • **vlan-fdb** If you do not specify a configuration area, nondefault information for all areas is displayed.
all	Includes configuration items that are set to their default values.

Defaults

None.

Mode

Enabled.

Usage

If you do not use one of the optional parameters, configuration commands that set nondefault values are displayed for all configuration areas. If you specify an area, commands are displayed for that area only. If you use the **all** option, the display also includes commands for configuration items that are set to their default values.

Example

The following command shows configuration information for VLANs:

```
RBT-8100# show config area vlan
# Configuration nvgen'd at 2004-5-21 19:36:48
# Image 3.0.0
# Model RBT-8100
# Last change occurred at 2004-5-21 18:20:50
set vlan 1 port 1
```

Related Commands

- load config on page 20-11
- save config on page 20-20

show version

Displays software and hardware version information for a RoamAbout switch and, optionally, for any attached access points.

Syntax

show version [**details**]

Parameters

details	Includes additional software build information and information about the access points configured on the RoamAbout switch.

Defaults

None

Mode

All.

Example

The following command displays version information for a RoamAbout switch:

```
RBT-8100# show version

        Mobility System Software, Version: 3.0.0
        Copyright (c) 2003,2004 by Enterasys Networks, Inc

Build Information: (build#75) TOP 2004-06-30 07:25:00
Model:             RBT-8100
Hardware
   Mainboard:      version 0 ; FPGA version 0
   PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
Flash:             3.0.0.375  - md0a
Kernel:            3.0.0#43: Wed Jun 30 05:17:44 PDT 2004
BootLoader:        1.19 / 1.7.4
```

The following command displays additional software build information and access point information:

```
RBT-8100# show version details

        Mobility System Software, Version: 3.0.0
        Copyright (c) 2003,2004 by Enterasys Networks, Inc

Build Information: (build#75) TOP 2004-06-30 07:25:00
Model:             RBT-8100
Hardware
   Mainboard:      version 0 ; FPGA version 0
   PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
```

```
Flash:              3.0.0.375  - md0a
Kernel:             3.0.0#43: Wed Jun 30 05:17:44 PDT 2004
BootLoader:         1.19 / 1.7.4

Port/DAP AP Model   Serial #    Versions
-------- ---------- ----------- ------------------------
-   /23  AP3000 0123456789  H/W  : A3
                            F/W1 : 5.6
                            F/W2 : 5.6
                            S/W  : 3.0.0
-   /24  AP3000 9876543210  H/W  : A3
                            F/W1 : 5.6
                            F/W2 : N/A
                            S/W  : 3.0.0
```

Table 20-3 describes the fields in the **show version** output.

Table 20-3 Output for show version

Output	What It Displays...
Build Information	Factory timestamp of the image file.
Label	Software version and build date.
Build Suffix	Build suffix.
Model	Build model.
Hardware	Version information for the RoamAbout switch's motherboard and Power over Ethernet (PoE) board.
Serial number	Serial number of the RoamAbout switch.
Flash	Flash memory version.
Kernel	Kernel version.
BootLoader	Boot code version.
Port/DAP	Port number connected to an access point.
AP Model	AP model number.
Serial #	AP serial number.
Versions	AP hardware, firmware, and software versions.

Related Commands

show boot on page 20-24

uninstall soda agent

Removes the contents of a directory containing SODA agent files.

uninstall soda agent agent-directory *directory*

Parameters

directory	Directory on the RoamAbout Switch where SODA agent files are to be removed.

Defaults

None.

Mode

Enabled.

Usage

Use this command to remove a SODA agent directory and all of its contents. All files in the specified directory are removed. The command removes the directory and its contents, regardless of whether it contains SODA agent files.

Example

The following command removes the directory *sp1* and all of its contents:

```
RBT-8100# uninstall soda agent agent-directory sp1
This will delete all files in agent-directory, do you wish to continue? (y|n)
[n]y
```

Related Commands

- install soda agent on page 20-10
- set service-profile soda mode on page 11-110

21

Trace Commands

Use trace commands to perform diagnostic routines. While MSS allows you to run many types of traces, this chapter describes commands for those traces you are most likely to use. For a complete listing of the types of traces MSS allows, type the **set trace ?** command.

Caution: Using the **set trace** command can have adverse effects on system performance. Enterasys Networks, Inc. recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.

This chapter presents trace commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear log trace	21-2
clear trace	21-3
save trace	21-4
set trace authentication	21-5
set trace authorization	21-6
set trace dot1x	21-7
set trace sm	21-8
show trace	21-9

clear log trace

Deletes the log messages stored in the trace buffer.

Syntax

```
clear log trace
```

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

To delete the trace log, type the following command:

```
RBT-8100# clear log trace
```

Related Commands

- set log on page 23-3
- show log buffer on page 23-7

clear trace

Deletes running trace commands and ends trace processes.

Syntax

clear trace {*trace-area* | **all**}

Parameters

trace-area	Ends a particular trace process. Specify one of the following keywords to end the traces documented in this chapter: • **authorization**—Ends an authorization trace • **dot1x**—Ends an 802.1X trace • **authentication**—Ends an authentication trace • **sm**—Ends a session manager trace
all	Ends all trace processes.

Defaults

None.

Mode

Enabled.

Example

To clear all trace processes, type the following command:

```
RBT-8100# clear trace all
success: clear trace all
```

To clear the session manager trace, type the following command:

```
RBT-8100# clear trace sm
success: clear trace sm
```

Related Commands

- set trace authentication on page 21-5
- set trace authorization on page 21-6
- set trace dot1x on page 21-7
- set trace sm on page 21-8
- show trace on page 21-9

save trace

Saves the accumulated trace data for enabled traces to a file in the RoamAbout switch's nonvolatile storage.

Syntax

```
save trace filename
```

Parameters

filename	Name for the trace file. To save the file in a subdirectory, specify the subdirectory name, then a slash. For example: **traces/trace1**

Defaults

None.

Mode

Enabled.

Example

To save trace data into the file *trace1* in the subdirectory *traces*, type the following command:

```
RBT-8100# save trace traces/trace1
```

set trace authentication

Traces authentication information.

Syntax

set trace authentication [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

Parameters

mac-addr *mac-address*	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port *port-num*	Traces a port number. Specify a RoamAbout switch port number between 1 and 22.
user *username*	Traces a user. Specify a username of up to 32 alphanumeric characters with no spaces.
level *level*	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults

The default trace level is 5.

Mode

Enabled.

Example

The following command starts a trace for information about user *jose's* authentication:

```
RBT-8100# set trace authentication user jose
success: change accepted.
```

Related Commands

- clear trace on page 21-3
- show trace on page 21-9

set trace authorization

Traces authorization information.

Syntax

set trace authorization [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

Parameters

mac-addr *mac-address*	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port *port-num*	Traces a port number. Specify a RoamAbout switch port number between 1 and 22.
user *username*	Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
level *level*	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults

The default trace level is 5.

Mode

Enabled.

Example

The following command starts a trace for information for authorization for MAC address 00:01:02:03:04:05:

```
RBT-8100# set trace authorization mac-addr 00:01:02:03:04:05
success: change accepted.
```

Related Commands

- clear trace on page 21-3
- show trace on page 21-9

set trace dot1x

Traces 802.1X sessions.

Syntax

set trace dot1x [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

Parameters

mac-addr *mac-address*	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port *port-num*	Traces a port number. Specify a RoamAbout switch port number between 1 and 22.
user *username*	Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
level *level*	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults

The default trace level is 5.

Mode

Enabled.

Example

The following command starts a trace for the 802.1X sessions for MAC address 00:01:02:03:04:05:

```
RBT-8100# set trace dot1x mac-addr 00:01:02:03:04:05:
success: change accepted.
```

Related Commands

- clear trace on page 21-3
- show trace on page 21-9

set trace sm

Traces session manager activity.

Syntax

set trace sm [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

Parameters

mac-addr *mac-address*	Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
port *port-num*	Traces a port number. Specify a RoamAbout switch port number between 1 and 22.
user *username*	Traces a user. Specify a username of up to 80 alphanumeric characters, with no spaces.
level *level*	Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults

The default trace level is 5.

Mode

Enabled.

Example

Type the following command to trace session manager activity for MAC address 00:01:02:03:04:05:

```
RBT-8100# set trace sm mac-addr 00:01:02:03:04:05:
success: change accepted.
```

Related Commands

- clear trace on page 21-3
- show trace on page 21-9

show trace

Displays information about traces that are currently configured on the RoamAbout switch, or all possible trace options.

Syntax

show trace [**all**]

Parameters

all	Displays all possible trace options and their configuration.

Defaults

None.

Mode

Enabled.

Example

To view the traces currently running, type the following command:

```
RBT-8100# show trace
milliseconds spent printing traces: 1885.614
Trace Area           Level Mac               User              Port Filter
-------------------- ----- ----------------- ----------------- ---- --------
dot1x                    5                                              0
sm                       5                                              0
```

Related Commands

- clear trace on page 21-3
- set trace authentication on page 21-5
- set trace authorization on page 21-6
- set trace dot1x on page 21-7
- set trace sm on page 21-8

22

Snoop Commands

Use snoop commands to monitor wireless traffic, by using a Distributed AP (DAP) as a sniffing device. The DAP copies the sniffed 802.11 packets and sends the copies to an observer, which is typically a protocol analyzer such as Ethereal or Tethereal.

For more information, including setup instructions for the monitoring station, refer to the "Remote Monitoring Traffic" section in the "Troubleshooting a RoamAbout Switch" chapter of the *RoamAbout Mobility System Software Configuration Guide*.

This chapter presents snoop commands alphabetically. Use the following table to locate commands in this chapter.

For information about...	Refer to page...
clear snoop	22-2
clear snoop map	22-3
set snoop	22-4
set snoop map	22-6
set snoop mode	22-7
show snoop	22-8
show snoop info	22-9
show snoop map	22-10
show snoop stats	22-11

clear snoop

Deletes a snoop filter.

Syntax

clear snoop *filter-name*

Parameters

filter-name	Name of the snoop filter.

Defaults

None.

Mode

Enabled.

Example

The following command deletes snoop filter *snoop1*:

```
RBT-8100# clear snoop snoop1
```

Related Commands

- set snoop on page 22-4
- show snoop info on page 22-9

clear snoop map

Removes a snoop filter from an DAP radio.

Syntax

clear snoop map *filter-name* **dap** *dap-num* **radio** {**1** | **2**}

filter-name	Name of the snoop filter.
dap *dap-num*	Number of a DAP to which to snoop filter is mapped.
radio 1	Radio 1 of the DAP.
radio 2	Radio 2 of the DAP. (This option does not apply to single-radio models.)

Defaults

None.

Mode

Enabled.

Examples

The following command removes snoop filter *snoop2* from radio 2 on DAP 3:

```
RBT-8100# clear snoop map snoop2 dap 3 radio 2
success: change accepted.
```

The following command removes all snoop filter mappings from all radios:

```
RBT-8100# clear snoop map all
success: change accepted.
```

Related Commands

- set snoop map on page 22-6
- show snoop on page 22-8
- show snoop map on page 22-10

set snoop

Configures a snoop filter.

Syntax

set snoop *filter-name* [*condition-list*] [**observer** *ip-addr*] [**snap-length** *num*]

Parameters

filter-name	Name for the filter. The name can be up to 15 alphanumeric characters, with no spaces.
condition-list	Match criteria for packets. Conditions in the list are ANDed. Therefore, to be copied and sent to an observer, a packet must match all criteria in the *condition-list*. You can specify up to eight of the following conditions in a filter, in any order or combination: **frame-type** {**eq** | **neq**} {**beacon** | **control** | **data** | **management** | **probe**} **channel** {**eq** | **neq**} *channel* **bssid** {**eq** | **neq**} *bssid* **src-mac** {**eq** | **neq** | **lt** | **gt**} *mac-addr* **dest-mac** {**eq** | **neq** | **lt** | **gt**} *mac-addr* **host-mac** {**eq** | **neq** | **lt** | **gt**} *mac-addr* To match on packets to or from a specific MAC address, use the **dest-mac** or **src-mac** option. To match on both send and receive traffic for a host address, use the **host-mac** option. To match on a traffic flow (source and destination MAC addresses), use the **mac-pair** option. This option matches for either direction of a flow, and either MAC address can be the source or destination address. If you omit a condition, all packets match that condition. For example, if you omit **frame-type**, all frame types match the filter. For most conditions, you can use **eq** (equal) to match only on traffic that matches the condition value. Use **neq** (not equal) to match only on traffic that is not equal to the condition value. The **src-mac**, **dest-mac**, and **host-mac** conditions also support **lt** (less than) and **gt** (greater than).
observer *ip-addr*	Specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the DAP radio still counts the packets that match the filter.
snap-length *num*	Specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. Enterasys Networks recommends specifying a snap length of 100 bytes or less.

Defaults

No snoop filters are configured by default.

Mode

Enabled.

Usage

Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

For best results:

- Do not specify an observer that is associated with the DAP where the snoop filter is running. This configuration causes an endless cycle of snoop traffic.
- If the snoop filter is running on a Distributed DAP, and the DAP used a DHCP server in its local subnet to configure its IP information, and the DAP did not receive a default router (gateway) address as a result, the observer must also be in the same subnet. Without a default router, the DAP cannot find the observer.
- The DAP that is running a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the DAP to the observer. If the observer is not present, the DAP still sends the snoop packets, which use bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the DAP. These ICMP messages can affect network and DAP performance.

Examples

The following command configures a snoop filter named *snoop1* that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
RBT-8100# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

The following command configures a snoop filter named *snoop2* that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
RBT-8100# set snoop snoop2 frame-type eq data mac-pair aa:bb:cc:dd:ee:ff
11:22:33:44:55:66 observer 10.10.30.3 snap-length 100
```

Related Commands

- clear snoop on page 22-2
- set snoop map on page 22-6
- set snoop mode on page 22-7
- show snoop info on page 22-9
- show snoop stats on page 22-11

set snoop map

Maps a snoop filter to a radio on a DAP. A snoop filter does take effect until you map it to a radio and enable the filter.

Syntax

set snoop map *filter-name* **dap** *dap-num* **radio** {**1** | **2**}

filter-name	Name of the snoop filter.
dap *dap-num*	Number of a DAP to which to map the snoop filter.
radio 1	Radio 1 of the DAP.
radio 2	Radio 2 of the DAP. (This option does not apply to single-radio models.)

Defaults

Snoop filters are unmapped by default.

Mode

Enabled.

Usage

You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the DAP sends only one copy of a packet that matches a filter to the observer. After the first match, the DAP sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the DAP still maintains a counter of the number of packets that match the filter. (See show snoop stats on page 22-11.)

Example

The following command maps snoop filter *snoop1* to radio 2 on DAP 3:

```
RBT-8100# set snoop map snoop1 dap 3 radio 2
success: change accepted.
```

Related Commands

- clear snoop map on page 22-3
- set snoop on page 22-4
- set snoop mode on page 22-7
- show snoop map on page 22-10
- show snoop stats on page 22-11

set snoop mode

Enables a snoop filter. A snoop filter does not take effect until you map it to an DAP radio and enable the filter.

Syntax

set snoop {*filter-name* | **all**} **mode** {**enable** [**stop-after** *num-pkts*] | **disable**}

filter-name | **all**}	Name of the snoop filter. Specify all to enable all snoop filters.
enable [**stop-after** *num-pkts*]	Enables the snoop filter. The **stop-after** option disables the filter after the specified number of packets match the filter. Without the **stop-after** option, the filter operates until you disable it or until the DAP is restarted.
disable	Disables the snoop filter.

Defaults

Snoop filters are disabled by default.

Mode

Enabled.

Usage

The filter mode is not retained if you change the filter configuration or disable and reenable the radio, or when the DAP or the RoamAbout Switch is restarted. You must reenable the filter to place it back into effect.

Example

The following command enables snoop filter *snoop1*, and configures the filter to stop after 5000 packets match the filter:

```
RBT-8100# set snoop snoop1 mode enable stop-after 5000
success: filter 'snoop1' enabled
```

Related Commands

- show snoop on page 22-8
- show snoop info on page 22-9
- show snoop map on page 22-10
- show snoop stats on page 22-11

show snoop

Displays the DAP radio mapping for all snoop filters.

Syntax

show snoop

Defaults

None.

Mode

Enabled.

Usage

To display the mappings for a specific DAP radio, use the **show snoop map** command.

Example

The following command shows the DAP radio mappings for all snoop filters configured on an RoamAbout Switch:

```
RBT-8100# show snoop
Dap: 3          Radio: 2
        snoop1
        snoop2
Dap: 2          Radio: 2
        snoop2
```

Related Commands

- clear snoop map on page 22-3
- set snoop map on page 22-6
- show snoop map on page 22-10

show snoop info

Shows the configured snoop filters.

Syntax

show snoop *filter-name*

filter-name	Name of the snoop filter.

Defaults

None.

Mode

Enabled.

Example

The following command shows the snoop filters configured in the examples above:

```
RBT-8100# show snoop info
snoop1:
        observer 10.10.30.2 snap-length 100
        all packets
snoop2:
        observer 10.10.30.3 snap-length 100
        frame-type eq data
        mac-pair (aa:bb:cc:dd:ee:ff, 11:22:33:44:55:66)
```

Related Commands

- clear snoop on page 22-2
- set snoop on page 22-4

show snoop map

Shows the DAP radios that are mapped to a specific snoop filter.

Syntax

show snoop map *filter-name*

filter-name	Name of the snoop filter.

Defaults

None.

Mode

Enabled.

Usage

To display the mappings for all snoop filters, use the **show snoop** command.

Example

The following command shows the mapping for snoop filter *snoop1*:

```
RBT-8100# show snoop map snoop1
filter 'snoop1' mapping
        Dap: 3          Radio: 2
```

Related Commands

- clear snoop map on page 22-3
- set snoop map on page 22-6
- show snoop on page 22-8

show snoop stats

Displays statistics for enabled snoop filters.

Syntax

show snoop stats [*filter-name* [*dap-num* [**radio** {**1** | **2**}]]]

filter-name	Name of the snoop filter.
dap *dap-num*	Number of a DAP to which the snoop filter is mapped.
radio 1	Radio 1 of the DAP.
radio 2	Radio 2 of the DAP. (This option does not apply to single-radio models.)

Defaults

None.

Mode

Enabled.

Usage

The DAP retains statistics for a snoop filter until the filter is changed or disabled. The DAP then clears the statistics.

Example

The following command shows statistics for snoop filter *snoop1*:

```
RBT-8100# show snoop stats snoop1
Filter          Dap Radio   Rx Match     Tx Match     Dropped        Stop-After
================================================================================
snoop1            3     1            96           4            0      stopped
```

Table 22-1 describes the fields in this display.

Table 22-1 show snoop stats Output

Field	Description
Filter	Name of the snoop filter.
Dap	DAP containing the radio to which the filter is mapped.
Radio	Radio to which the filter is mapped.
Rx Match	Number of packets received by the radio that match the filter.
Tx Match	Number of packets sent by the radio that match the filter.
Dropped	Number of packets that matched the filter but that were not copied to the observer due to memory or network problems.
Stop-After	Filter state: running—enabled stopped—disabled *number-of-packets*—If the filter is running and the stop-after option was used to stop the filter, this field displays the number of packets that still need to match before the filter is stopped.

23

System Log Commands

Use the system log commands to record information for monitoring and troubleshooting. MSS system logs are based on RFC 3164, which defines the log protocol.

This chapter presents system log commands alphabetically. Use the following table to locate commands in this chapter based on their use.

For information about...	Refer to page...
clear log	23-2
set log	23-3
set log mark	23-6
show log buffer	23-7
show log config	23-9
show log trace	23-10

clear log

Clears the log messages stored in the log buffer, or removes the configuration for a syslog server and stops sending log messages to that server.

Syntax

clear log [**buffer** | **server** *ip-addr*]

Parameters

buffer	Deletes the log messages stored in nonvolatile storage.
server *ip-addr*	Deletes the configuration for and stops sending log messages to the syslog server at this IP address. Specify an address in dotted decimal notation.

Defaults

None.

Mode

Enabled.

Examples

To stop sending system logging messages to a server at 192.168.253.11, type the following command:

```
RBT-8100# clear log server 192.168.253.11
success: change accepted.
```

Type the following command to clear all messages from the log buffer:

```
RBT-8100# clear log buffer
success: change accepted.
```

Related Commands

- clear log trace on page 21-2
- set log on page 23-3

set log

Enables or disables logging of RoamAbout switch and AP events to the RoamAbout switch log buffer or other logging destination and sets the level of the events logged. For logging to a syslog server only, you can also set the facility logged.

Syntax

set log {**buffer** | **console** | **current** | **sessions** | **trace**} [**severity** *severity-level*] [**enable** | **disable**]

set log server *ip-addr* [**port** *port-number*] **severity** *severity-level* [**local-facility** *facility-level*]

Parameters

buffer	Sets log parameters for the log buffer in nonvolatile storage.
console	Sets log parameters for console sessions.
current	Sets log parameters for the current Telnet or console session. These settings are not stored in nonvolatile memory.
server *ip-addr*	Sets log parameters for a syslog server. Specify an address in dotted decimal notation.
sessions	Sets the default log values for Telnet sessions. You can set defaults for the following log parameters: Severity Logging state (enabled or disabled) To override the session defaults for an individual session, type the **set log** command from within the session and use the **current** option.
trace	Sets log parameters for trace files.
port *port-number*	Sets the TCP port for sending messages to the syslog server. You can specify a number from 1 to 65535. The default syslog port is 514.
severity *severity-level*	Logs events at a severity level greater than or equal to the level specified. Specify one of the following: • **emergency**—The RoamAbout switch is unusable. • **alert**—Action must be taken immediately. • **critical**—You must resolve the critical conditions. If the conditions are not resolved, the RoamAbout switch can reboot or shut down. • **error**—The RoamAbout switch is missing data or is unable to form a connection. • **warning**—A possible problem exists. • **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required. • **info**—Informational messages only. No problem exists. • **debug**—Output from debugging.

local-facility *facility-level*	For messages sent to a syslog server, maps all messages of the severity you specify to one of the standard local log facilities defined in RFC 3164. You can specify one of the following values: • **0**—maps all messages to *local0*. • **1**—maps all messages to *local1*. • **2**—maps all messages to *local2*. • **3**—maps all messages to *local3*. • **4**—maps all messages to *local4*. • **5**—maps all messages to *local5*. • **6**—maps all messages to *local6*. • **7**—maps all messages to *local7*. If you do not specify a local facility, MSS sends the messages with their default MSS facilities. For example, AAA messages are sent with facility 4 and boot messages are sent with facility 20 by default.
enable	Enables messages to the specified target.
disable	Disables messages to the specified target.

Defaults

- Events at the error level and higher are logged to the RoamAbout switch console.
- Events at the error level and higher are logged to the RoamAbout switch system buffer.
- Trace logging is enabled, and debug-level output is stored in the RoamAbout switch trace buffer.

Mode

Enabled.

Usage

Using the command with only enable or disable turns logging on or off for the target at all levels. For example, entering set log buffer enable with no other keywords turns on logging to the system buffer of all facilities at all levels. Entering set log buffer disable with no other keywords turns off all logging to the buffer.

Example

To log only emergency, alert, and critical system events to the console, type the following command:

```
RBT-8100# set log console severity critical enable
success: change accepted.
```

Related Commands

- show log config on page 23-9
- clear log on page 23-2

set log mark

Configures MSS to generate mark messages at regular intervals. The mark messages indicate the current system time and date. Enterasys Networks can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

Syntax

set log mark [**enable** | **disable**] [**severity** *level*]
[**interval** *interval*]

Parameters

enable	Enables the mark messages.
disable	Disables the mark messages.
severity *level*	Log severity at which the messages are logged: • **emergency** • **alert** • **critical** • **error** • **warning** • **notice** • **info** • **debug**
interval *interval*	Interval at which MSS generates the mark messages. You can specify from 1 to 2147483647 seconds.

Defaults

Mark messages are disabled by default. When they are enabled, MSS generates a message at the notice level once every 300 seconds by default.

Mode

Enabled.

Example

The following command enables mark messages:

```
RBT-8100# set log mark enable
success: change accepted.
```

show log buffer

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax

show log buffer [{**+**|**-**}*number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

Parameters

buffer	Displays the log messages in nonvolatile storage.
+|-*number-of-messages*	Displays the number of messages specified as follows: • A positive number (for example, **+100**), displays that number of log entries starting from the oldest in the log. • A negative number (for example, **-100**) displays that number of log entries starting from newest in the log.
facility *facility-name*	Area of MSS that is sending the log message. Type a space and a question mark (**?**) after s**how log buffer facility** for a list of valid facilities.
matching *string*	Displays messages that match a string—for example, a username or IP address.
severity *severity-level*	Displays messages at a severity level greater than or equal to the level specified. Specify one of the following: • **emergency**—The RoamAbout switch is unusable. • **alert**—Action must be taken immediately. • **critical**—You must resolve the critical conditions. If the conditions are not resolved, the RoamAbout switch can reboot or shut down. • **error**—The RoamAbout switch is missing data or is unable to form a connection. • **warning—**A possible problem exists. • **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required. • **info**—Informational messages only. No problem exists. • **debug**—Output from debugging.

Defaults

None.

Mode

Enabled.

Usage

The debug level produces a lot of messages, many of which can appear to be somewhat cryptic. Debug messages are used primarily by Enterasys Networks for troubleshooting and are not intended for administrator use.

Examples

Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
RBT-8100# show log buffer facility ?
```

<facility name> Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP, ASO, BOOT, CLI, CLUSTER, CRYPTO, DOT1X, NET, ETHERNET, GATEWAY, HTTPD, IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE, SYS, TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, AP, RAPDA, WEBVIEW, EAP, FP, STAT, SSHD, SUP, DNSD, CONFIG, BACKUP.

The following command displays logged messages for the AAA facility:

```
RBT-8100# show log buffer facility AAA
AAA Jun. 25 09:11:32.579848 ERROR AAA_NOTIFY_ERR: AAA got SM special event (98)
on locality 3950 which is gone
```

Related Commands

- clear log on page 23-2
- show log config on page 23-9

show log config

Displays log configuration information.

Syntax

show log config

Parameters

None.

Defaults

None.

Mode

Enabled.

Example

To display how logging is configured, type the following command:

```
RBT-8100# show log config
Logging console:               disabled
Logging console severity:      DEBUG
Logging sessions:              disabled
Logging sessions severity:     INFO
Logging buffer:                enabled
Logging buffer severity:       WARNING
Logging trace:                 enabled
Logging trace severity:        DEBUG
Logging buffer size:           10485760 bytes
Log marking:                   disabled
Log marking severity:          NOTICE
Log marking interval:          300 seconds

Logging server:                10.1.1.10       severity EMERGENCY

Current session:                 disabled
Current session severity:        INFO
```

Related Commands

- set log on page 23-3
- clear log on page 23-2

show log trace

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax

show log trace [{**+**|**-**|**/**}*number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

Parameters

trace	Displays the log messages in the trace buffer.
+|-|/*number-of-messages*	Displays the number of messages specified as follows: • A positive number (for example, **+100**), displays that number of log entries starting from the oldest in the log. • A negative number (for example, **-100**) displays that number of log entries starting from newest in the log. • A number preceded by a slash (for example, **/100**) displays that number of the most recent log entries in the log, starting with the least recent.
facility *facility-name*	Area of MSS that is sending the log message. Type a space and a question mark **(?)** after **show log trace facility** for a list of valid facilities.
matching *string*	Displays messages that match a string—for example, a username or IP address.
severity *severity-level*	Displays messages at a severity level greater than or equal to the level specified. Specify one of the following: • **emergency**—The RoamAbout switch is unusable. • **alert**—Action must be taken immediately. • **critical**—You must resolve the critical conditions. If the conditions are not resolved, the RoamAbout switch can reboot or shut down. • **error**—The RoamAbout switch is missing data or is unable to form a connection. • **warning**—A possible problem exists. • **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required. • **info**—Informational messages only. No problem exists. • **debug**—Output from debugging.

Defaults

None.

Mode

Enabled.

Example

Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
RBT-8100# show log trace facility ?
<facility name>             Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP,
ASO, BOOT, CLI, CLUSTER, CRYPTO, DOT1X, ENCAP, ETHERNET, GATEWAY, HTTPD, IGMP,
IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE, SYS,
TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, AP, RAPDA,
WEBVIEW, EAP, PORTCONFIG, FP.
```

The following command displays the newest five trace log entries for the ROGUE facility:

```
RBT-8100# show log trace +5 facility ROGUE
ROGUE Oct 28 16:30:19.695141 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:ff:00:3b Po
rt 7 Radio 1 Chan 36 RSSI 18 Tech DOT_11A SSID Enterasys
                                                    ROGUE Oct 28 16:30:19.7046
37 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:00:09:5f Port 7 Radio 1 Chan 36 RSSI
15 Tech DOT_11A SSID examplewlan
                                ROGUE Oct 28 16:30:19.711253 ERROR ROGUE_AP_ALER
T: Xmtr Mac 01:0b:0e:00:06:b7 Port 7 Radio 1 Chan 36 RSSI 36 Tech DOT_11A SSID
wlan-7
       ROGUE Oct 28 16:30:19.717954 ERROR ROGUE_AP_ALERT: Xmtr Mac 00:0b:0e:00:0
6:8f Port 7 Radio 1 Chan 36 RSSI 13 Tech DOT_11A SSID Enterasys
                                                          ROGUE Oct 28 16:30:
19.727069 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:da:da:dd Port 7 Radio 1 Chan 3
6 RSSI 22 Tech DOT_11A SSID Enterasys
```

Related Commands

- clear log on page 23-2
- show log config on page 23-9

24

Boot Prompt Commands

Boot prompt commands enable you to perform basic tasks, including booting a system image file, from the boot prompt (boot>). A CLI session enters the boot prompt if MSS does not boot successfully or you intentionally interrupt the boot process. To interrupt the boot process, press **q** followed by **Enter** (return).

Caution: Generally, boot prompt commands are used only for troubleshooting. Enterasys Networks, Inc. recommends that you use these commands only when working with Enterasys Networks to diagnose a system issue. In particular, commands that change boot parameters can interfere with a RoamAbout switch's ability to boot successfully.

This chapter presents boot prompt commands alphabetically. Use the following table to locate commands in this chapter based on their use.

For information about...	Refer to page...
autoboot	24-2
boot	24-3
change	24-5
create	24-6
delete	24-7
dhcp	24-8
diag	24-9
dir	24-10
fver	24-11
help	24-12
ls	24-13
next	24-14
reset	24-15
show	24-16
test	24-18
version	24-19

autoboot

Displays or changes the state of the autoboot option. The autoboot option controls whether a RoamAbout switch automatically boots a system image after initializing the hardware, following a system reset or power cycle.

Syntax

autoboot [**ON** | **on** | **OFF** | **off**]

Parameters

ON	Enables the autoboot option.
on	Same effect as **ON**.
OFF	Disables the autoboot option.
off	Same effect as **OFF**.

Defaults

The autoboot option is enabled by default.

Mode

Boot prompt.

Example

The following command displays the current setting of the autoboot option:

```
boot> autoboot
The autoboot flag is on.
```

Related Commands

boot on page 24-3

boot

Loads and executes a system image file.

Syntax

boot [**BT=***type*] [**DEV=***device*] [**FN=***filename*] [**HA=***ip-addr*] [**FL=***num*] [**OPT=***option*] [**OPT+=***option*]

Parameters

BT=*type*	Boot type: • **c**—Compact flash. Boots using nonvolatile storage or a flash card. • **n**—Network. Boots using a TFTP server.
DEV=*device*	Location of the system image file: • **c:**—Nonvolatile storage area containing boot partition 0 • **d:**—Nonvolatile storage area containing boot partition 1 • **e:**—Primary partition of the flash card in the flash card slot • **f:**—Secondary partition of the flash card in the flash card slot • **boot0**—boot partition 0 • **boot1**—boot partition 1
FN=*filename*	System image filename.
HA=*ip-addr*	Host address (IP address) of a TFTP server. This parameter applies only when the boot type is **n** (network).
FL=*num*	Number representing the bit settings of boot flags to pass to the booted system image. Use this parameter only if advised to do so by Enterasys Networks.
OPT=*option*	String up to 128 bytes of boot options to pass to the booted system image *instead of* the boot option(s) in the currently active boot profile. The options temporarily replace the options in the boot profile. Use this parameter only if advised to do so by Enterasys Networks.
OPT+=*option*	String up to 128 bytes of boot options to pass to the booted system image *in addition to* the boot option(s) in the currently active boot profile. The options are appended to the options already in the boot profile. Use this parameter only if advised to do so by Enterasys Networks.

Defaults

The boot settings in the currently active boot profile are used by default.

Mode

Boot prompt.

Usage

If you use an optional parameter, the parameter setting overrides the setting of the same parameter in the currently active boot profile. However, the boot profile itself is not changed. To display the currently active boot profile, use the **show** command. To change the currently active boot profile, use the **change** command.

Example

The following command loads system image file RBT010101.020 from boot partition 1:

```
boot> boot FN=RBT010101.020 DEV=boot1
Compact Flash load from boot1:testcfg matches RBT010101.020.
unzip: Inflating ramdisk_1.1.1.. OK
unzip file len 36085486 OK


Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003
    The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California.  All rights reserved.

Power Cycle Reboot
Detecting hardware...done.
readclock: 2003-10-8 2:9:50.67 UTC=>1065578990.670000 (1064992894)
init: Creating mfs /dev
erase ^H, werase ^W, kill ^U, intr ^C, status ^T
Doing EnteRASys mounts and links
Starting nos_mon...
        nos_mon:ps: not found
SYSLOGD Oct 08 02:10:05.477814 CRITICAL SYSTEM_READY: The system has finished
booting.

Copyright (c) 2002, 2003
Enterasys Networks, Inc.

Username:
Password:
```

Related Commands

- change on page 24-5
- show on page 24-16

change

Changes parameters in the currently active boot profile. (For information about boot profiles, see show on page 24-16.)

Syntax

```
change
```

Parameters

None.

Defaults

The default boot type is **c** (compact flash). The default filename is *default*. The default flags setting is 0x00000000 (all flags disabled) and the default options list is run=nos;boot=0. The default device setting is the boot partition specified by the most recent **set boot partition** command typed at the Enabled level of the CLI, or boot 0 if the command has never been typed.

Mode

Boot prompt.

Usage

After you type the **change** command, the system interactively displays the current setting of each parameter and prompts you for the new setting. When prompted, type the new setting, press Enter to accept the current setting, or type **.** (period) to change the setting to its default value. To back up to the previous parameter, type **-** (hyphen).

For information about each of the boot parameters you can set, see show on page 24-16.

Example

The following command enters the configuration mode for the currently active boot profile, changes the device to **boot1, and leaves the other parameters with their current settings**:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)
BOOT TYPE:    [c]
DEVICE:       [boot0:]boot1
FILENAME:     [default]
FLAGS:        [0x00000000]
OPTIONS:      [run=nos;boot=0]
```

Related Commands

- boot on page 24-3
- create on page 24-6
- delete on page 24-7
- dhcp on page 24-8
- next on page 24-14
- show on page 24-16

create

Creates a new boot profile. (For information about boot profiles, see show on page 24-16.)

Syntax

create

Parameters

None.

Defaults

The new boot profile has the same settings as the currently active boot profile by default.

Mode

Boot prompt.

Usage

A RoamAbout switch can have up to four boot profiles. The boot profiles are stored in slots, numbered 0 through 3. When you create a new profile, the system uses the next available slot for the profile. If all four slots already contain profiles and you try to create a fifth profile, the switch displays a message advising you to change one of the existing profiles instead.

To make a new boot profile the currently active boot profile, use the **next** command. To change boot parameter settings, use the **change** command.

Example

The following command creates a new boot profile in slot 1 on a RoamAbout switch that currently has only one boot profile, in slot 0:

```
boot> create

    BOOT Index:   1
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

Related Commands

- change on page 24-5
- delete on page 24-7
- next on page 24-14
- show on page 24-16

delete

Removes the currently active boot profile. (For information about boot profiles, see show on page 24-16.)

Syntax

delete

Parameters

None.

Defaults

None.

Mode

Boot prompt.

Usage

When you type the **delete** command, the next-lower numbered boot profile becomes the active profile. For example, if the currently active profile is number 3, profile number 2 becomes active after you type **delete** to delete profile 3. You cannot delete boot profile 0.

Example

To remove the currently active boot profile, type the following command:

```
boot> delete

    BOOT Index:   1
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

Related Commands

- change on page 24-5
- create on page 24-6
- next on page 24-14
- show on page 24-16

dhcp

Displays or changes the state of the DHCP option. The DHCP option controls whether an RoamAbout switch uses DCHP to obtain its IP address when it is booted using a TFTP server.

Syntax

dhcp [**ON** | **on** | **OFF** | **off**]

Parameters

ON	Enables the DHCP option.
on	Same effect as **ON**.
OFF	Disables the DHCP option.
off	Same effect as **OFF**.

Defaults

The DHCP option is disabled by default.

Mode

Boot prompt.

Examples

The following command displays the current setting of the DHCP option:

```
boot> dhcp
DHCP is currently enabled.
```

The following command disables the DHCP option:

```
boot> dhcp
DHCP is currently disabled.
```

Related Commands

boot on page 24-3

diag

Accesses the diagnostic mode.

Syntax

```
diag
```

Parameters

None.

Defaults

The diagnostic mode is disabled by default.

Mode

Boot prompt.

Usage

Access to the diagnostic mode requires a password, which is not user configurable. Use this mode only if advised to do so by Enterasys Networks.

dir

Displays the boot code and system image files on a RoamAbout switch.

Syntax

dir [**c:** | **d:** | **e:** | **f:** | **boot0** | **boot1**]

Parameters

c:	Nonvolatile storage area containing boot partition 0 (primary).
d:	Nonvolatile storage area containing boot partition 1 (secondary).
e:	Primary partition of the flash card in the flash card slot.
f:	Secondary partition of the flash card in the flash card slot.
boot0	Boot partition 0.
boot1	Boot partition 1.

Defaults

None.

Mode

Boot prompt.

Usage

To display the system image software versions, use the **fver** command. This command does not list the boot code versions. To display the boot code versions, use the **version** command.

Example

The following command displays all the boot code and system image files on a RoamAbout switch:

```
boot> dir
  Internal Compact Flash Directory (Primary):
         RBT010101.020                5523634 bytes
               BLOAD                 696176 bytes
              BSTRAP                  38056 bytes
  Internal Compact Flash Directory (Secondary):
         RBT010101.020                5524593 bytes
```

Related Commands

- fver on page 24-11
- version on page 24-19

fver

Displays the version of a system image file installed in a specific location on a RoamAbout switch.

Syntax

fver {**c:** | **d:** | **e:** | **f:** | **boot0:** | **boot1:**} [*filename*]

Parameters

c:	Nonvolatile storage area containing boot partition 0 (primary).
d:	Nonvolatile storage area containing boot partition 1 (secondary).
e:	Primary partition of the flash card in the flash card slot.
f:	Secondary partition of the flash card in the flash card slot.
boot0:	Boot partition 0.
boot1:	Boot partition 1.
[*filename*]	System image filename.

Defaults

None.

Mode

Boot prompt.

Usage

To display the image filenames, use the **dir** command. This command does not list the boot code versions. To display the boot code versions, use the **version** command.

Example

The following command displays the system image version installed in boot partition 1:

```
boot> fver boot1
File boot1:default version is 1.1.0.98.
```

Related Commands

- dir on page 24-10
- version on page 24-19

help

Displays a list of all the boot prompt commands or detailed information for an individual command.

Syntax

help [*command-name*]

Parameters

command-name	Boot prompt command.

Defaults

None.

Mode

Boot prompt.

Usage

If you specify a command name, detailed information is displayed for that command. If you do not specify a command name, all the boot prompt commands are listed.

Example

The following command displays detailed information for the **fver** command:

```
boot> help fver

        fver  Display the version of the specified device:filename.

  USAGE:  fver [c:file|d:file|e:file|f:file|boot0:file|boot1:file|boot2:file|boo
t3:file]

    Command to display the version of the compressed image file
    associated with the given device:filename.
```

Related Commands

ls on page 24-13

ls

Displays a list of the boot prompt commands.

Syntax

ls

Parameters

None.

Defaults

None.

Mode

Boot prompt.

Usage

To display help for an individual command, type help followed by the command name (for example, **help boot**).

Example

To display a list of the commands available at the boot prompt, type the following command:

```
boot> ls
          ls     Display a list of all commands and descriptions.
        help     Display help information for each command.
    autoboot     Display the state of, enable, or disable the autoboot option.
        boot     Load and execute an image using the current boot configuration
profile.
      change     Change the current boot configuration profile.
      create     Create a new boot configuration profile.
      delete     Delete the current boot configuration profile.
        next     Select the next boot configuration profile.
        show     Display the current boot configuration profile.
         dir     Display the contents of the specified boot partition.
        fver     Display the version of the loadable image specified by
device:filename.
     version     Display HW and Bootstrap/Bootloader version information.
       reset     Reset the system.
        test     Display the state of, enable, or disable the tests option.
        diag     Access the diagnostic command CLI.
```

Related Commands

help on page 24-12

next

Activates and displays the boot profile in the next boot profile slot. (For information about boot profiles, see show on page 24-16.)

Syntax

next

Parameters

None.

Defaults

None.

Mode

Boot prompt.

Usage

A RoamAbout switch contains 4 boot profile slots, numbered 0 through 3. This command activates the boot profile in the next slot, in ascending numerical order. If the currently active slot is 3, the command activates the boot profile in slot 0.

Example

To activate the boot profile in the next slot and display the profile, type the following command:

```
boot> next

    BOOT Index:    0
    BOOT TYPE:     c
    DEVICE:        boot1:
    FILENAME:      testcfg
    FLAGS:         00000000
    OPTIONS:       run=nos;boot=0
```

Related Commands

- change on page 24-5
- create on page 24-6
- delete on page 24-7
- show on page 24-16

reset

Resets a RoamAbout switch's hardware.

Syntax

reset

Parameters

None.

Defaults

None.

Mode

Boot prompt.

Usage

After resetting the hardware, the reset command attempts to load a system image file only if other boot settings are configured to do so.

Example

To immediately reset the system, type the following command at the boot prompt:

```
boot> reset

Enterasys Networks RBTBootstrap 1.17 Release
Testing Low Memory 1 ............
Testing Low Memory 2 ............
CISTPL_VERS_1:  4.1   <SanDisk> <SDP> <5/3 0.6>
Reset Cause (0x02) is COLD

Enterasys Networks RBT Bootstrap/Bootloader
                  Version  1.6.5  Release
     Bootstrap 0 version:          1.17     Active
    Bootloader 0 version:         1.6.5     Active
     Bootstrap 1 version:          1.17
    Bootloader 1 version:         1.6.3

       RBT Board Revision:    3.
  RBT Controller Revision:    24.
      POE Board Revision:    1
 POE Controller Revision:    6
    BOOT Index:   0
    BOOT TYPE:    c
    DEVICE:       boot1:
    FILENAME:     default
    FLAGS:        00000000
    OPTIONS:      run=nos;boot=0
```

Related Commands

boot on page 24-3

show

Displays the currently active boot profile. A boot profile is a set of parameters that a RoamAbout switch uses to control the boot process. Each boot profile contains the following parameters:

- Boot type—Either compact flash (local device on the RoamAbout switch) or network (TFTP)
- Boot device—Location of the system image file
- Filename—System image file
- Flags—Number representing the bit settings of boot flags to pass to the booted system image.
- Options—String up to 128 bytes of boot options to pass to the booted system image

A RoamAbout switch can have up to four boot profiles, numbered 0 through 3. Only one boot profile can be active at a time. You can create, change, and delete boot profiles. You also can activate another boot profile in place of the currently active one.

Syntax

show

Parameters

None.

Defaults

None.

Mode

Boot prompt.

Example

To display the currently active boot profile, type the following command at the boot prompt:

```
boot> show

    BOOT Index:    0
    BOOT TYPE:     c
    DEVICE:        boot1:
    FILENAME:      default
    FLAGS:         00000000
    OPTIONS:       run=nos;boot=0
```

Table 24-1 describes the fields in the display.

Table 24-1 Output for show

Output	What It Displays...
BOOT Index	Boot profile slot, which can be a number from 0 to 3.
BOOT TYPE	Boot type: • **c**—Compact flash. Boots using nonvolatile storage or a flash card. • **n**—Network. Boots using a TFTP server.

Table 24-1 Output for show (continued)

Output	What It Displays...
DEVICE	Location of the system image file: • **c:**—Nonvolatile storage area containing boot partition 0 • **d:**—Nonvolatile storage area containing boot partition 1 • **e:**—Primary partition of the flash card in the flash card slot • **f:**—Secondary partition of the flash card in the flash card slot • **boot0**—boot partition 0 • **boot1**—boot partition 1
FILENAME	System image file name.
FLAGS	Number representing the bit settings of boot flags to pass to the booted system image.
OPTIONS	String up to 128 bytes of boot options to pass to the booted system image.

Related Commands

- change on page 24-5
- create on page 24-6
- delete on page 24-7
- next on page 24-14

test

Displays or changes the state of the poweron test flag. The poweron test flag controls whether a RoamAbout switch performs a set of self tests prior to the boot process.

Syntax

```
test [ON | on | OFF | off]
```

Parameters

ON	Enables the poweron test flag.
on	Same effect as **ON**.
OFF	Disables the poweron test flag.
off	Same effect as **OFF**.

Defaults

The poweron test flag is disabled by default.

Mode

Boot prompt.

Example

The following command displays the current setting of the poweron test flag:

```
boot> test
The diagnostic execution flag is not set.
```

Related Commands

- boot on page 24-3

version

Displays version information for a RoamAbout switch's hardware and boot code.

Syntax

version

Parameters

None.

Defaults

None.

Mode

Boot prompt.

Usage

This command does not list the system image file versions installed in the boot partitions. To display system image file versions, use the **dir** or **fver** command.

Example

To display hardware and boot code version information, type the following command at the boot prompt:

```
boot> version

Enterasys Networks RBT Bootstrap/Bootloader

                 Version  1.6.5  Release
    Bootstrap 0 version:          1.17     Active
   Bootloader 0 version:         1.6.5     Active
    Bootstrap 1 version:          1.17
   Bootloader 1 version:         1.6.3

      RBT Board Revision:    3.
 RBT Controller Revision:    24.
     POE Board Revision:    1
POE Controller Revision:    6
```

Related Commands

- dir on page 24-10
- fver on page 24-11

Index

A

access levels, command line 1-8
administrative access mode 1-1
all access 1-8
asterisks (*)
  in MAC addresses 1-3
  in user globs 1-4
asterisks. See double asterisks (**); single asterisks (*)

C

CIDR format for subnet masks in command entries 1-3
classless interdomain routing (CIDR) format 1-3
clear network-domain 10-2
clear port media-type 4-5
clear prompt 3-4
CLI (command-line interface)
  command description format 1-8
  command prompts 1-2
  conventions 1-1
  help 1-7
  history buffer command reuse 1-6
  keyboard shortcuts 1-6
  list formats 1-5
  MAC address globs 1-3
  overview 1-1
  port list conventions 1-5
  subnet mask notation 1-3
  syntax notation 1-2
  tabs for command completion 1-6
  text entry conventions 1-2
  user globs 1-3
  VLAN identification 1-5
  wildcard mask notation 1-3
command description format 1-8
command history description
  history, command 1-8
command prompts 1-2
command-line interface. See CLI (command-line interface)
connection modes, CLI 1-1
conventions, CLI 1-1

D

delimiter characters, for user globs 1-3
dotted decimal notation, in IP addresses 1-3
double asterisks (**)
  in user globs 1-3
  in VLAN globs 1-4
  wildcard 1-7

E

enabled access 1-8
Ethernet ports
  port list conventions 1-5

G

globs, VLAN
  defined 1-4
globs. See MAC address globs; user globs; VLAN globs

H

help, command-line 1-7
history buffer, reusing commands in 1-6

I

IP addresses
  conventions for entry and display 1-3

K

keyboard shortcuts for command entry 1-6

L

last-resort username
  passwords are invalid 8-55
list formats for command entry 1-5

M

MAC address 18-13
MAC address globs
  conventions for 1-4
  matching order 1-5
  single asterisks (*) in 1-4
  wildcards in 1-4
MAC addresses
  asterisks (*) in 1-3
  leading zeros in 1-3
  wildcards in 1-3
mobility domain member 9-4
Mobility System Software CLI. See CLI (command-line interface) 1-1, 2-1, 5-1
MSS CLI. See CLI (command-line interface)
Multicast packets 18-14

N

names
  globbing in 1-3
network access mode 1-1

O

online help, command line 1-7

P

password
  invalid for last-resort users 8-55
port lists
  conventions for 1-5

S

show port media-type 4-30
single asterisks (*)
  in MAC address globs 1-4
  in VLAN globs 1-4
  wildcard 1-7
subnet masks
  notation conventions 1-3
syntax notation 1-2

T

tabs, for command completion 1-6

U

unicast 18-13
Unicast bytes in 18-13
Unicast packets in 18-13
Unicast packets out 18-14
user globs
  asterisks (*) in 1-4
  conventions for 1-3
  delimiter characters 1-3
  double asterisks (**) in 1-3
  matching order 1-5
  wildcards in 1-4

V

virtual LANs. See VLANs (virtual LANs)
VLAN globs
  conventions for 1-4
  double asterisks (**) in 1-4
  matching order 1-5
  single asterisks (*) in 1-4
  wildcards in 1-4
VLAN ID or name 1-5
VLANs (virtual LANs)
  VLAN globs in mobility ACLs 1-4
  VLAN name or number 1-5
  VLAN names 1-5
  VLAN numbers 1-5

W

wildcard masks
  notation conventions 1-3
wildcards
  in MAC address globs 1-4
  in MAC addresses 1-3
  in user globs 1-4
  in VLAN globs 1-4

Command Index

A

autoboot 24-2

B

backup 20-2
boot 24-3

C

change 24-5
clear {ap | dap} radio 11-5
clear accounting 8-3
clear authentication admin 8-4
clear authentication console 8-5
clear authentication dot1x 8-6
clear authentication mac 8-7
clear authentication proxy 8-8
clear authentication web 8-9
clear banner motd 3-2
clear boot config 20-4
clear dap 4-2
clear dap boot-configuration 11-7
clear domain security 9-2
clear dot1x max-req 17-4
clear dot1x port-control 17-5
clear dot1x quiet-period 17-6
clear dot1x reauth-max 17-7
clear dot1x reauth-period 17-8
clear dot1x timeout auth-server 17-9
clear dot1x timeout supplicant 17-10
clear dot1x tx-period 17-11
clear fdb 5-2
clear history 3-3
clear igmp statistics 13-2
clear interface 7-4
clear ip alias 7-5
clear ip dns domain 7-6
clear ip dns server 7-7
clear ip route 7-8
clear ip telnet 7-9
clear location policy 8-10
clear log 23-2
clear log buffer 23-2
clear log server 23-2
clear log trace 21-2
clear mac-user 8-11
clear mac-user attr 8-12
clear mac-user group 8-13
clear mac-usergroup 8-14
clear mac-usergroup attr 8-15
clear mobility-domain 9-3
clear mobility-domain member 9-4
clear mobility-profile 8-16
clear network-domain 10-2
clear network-domain mode 10-3
clear network-domain peer 10-4
clear network-domain seed-ip 10-5
clear ntp server 7-10
clear ntp update-interval 7-11
clear port counters 4-3
clear port media-type 4-5
clear port mirror 4-6
clear port name 4-7
clear port type 4-8
clear port-group 4-4
clear prompt 3-4
clear qos 6-2
clear radio-profile 11-8
clear radius 16-2
clear radius client system-ip 16-4
clear radius proxy client 16-5
clear radius proxy port 16-6
clear radius server 16-7
clear rfdetect attack-list 19-3
clear rfdetect black-list 19-4
clear rfdetect countermeasures mac 19-5
clear rfdetect ignore 19-6
clear rfdetect ssid-list 19-7
clear rfdetect vendor-list 19-8
clear security acl 14-2
clear security acl map 14-4
clear security l2-restrict 5-4
clear security l2-restrict counters 5-5
clear server group 16-8
clear server group load-balance 16-8
clear service-profile 11-10
clear sessions 18-2
clear sessions network 18-3
clear snmp notify target 7-13
clear snmp profile 7-14
clear snmp trap receiver 7-15
clear snmp usm 7-16
clear snoop 22-2
clear snoop map 22-3
clear spantree portcost 12-2
clear spantree portpri 12-3
clear spantree portvlancost 12-4
clear spantree portvlanpri 12-5
clear spantree statistics 12-6
clear summertime 7-17
clear system 3-5
clear system countrycode 3-5
clear system ip-address 3-5, 7-18
clear system location 3-5
clear system name 3-5
clear timezone 7-19
clear trace 21-3
clear user 8-17
clear user attr 8-18
clear user group 8-19
clear usergroup 8-20
clear usergroup attr 8-21
clear vlan 5-6
commit security acl 14-6
copy 20-5
create 24-6
crypto ca-certificate 15-2
crypto ca-certificate admin 15-2
crypto ca-certificate eap 15-2
crypto certificate 15-4
crypto certificate admin 15-4
crypto certificate eap 15-4
crypto generate key 15-6
crypto generate request 15-7
crypto generate request admin 15-7
crypto generate request eap 15-7
crypto generate self-signed 15-9
crypto generate self-signed admin 15-9
crypto generate self-signed eap 15-9
crypto otp 15-11
crypto otp admin 15-11
crypto otp eap 15-11
crypto pkcs12 15-13
crypto pkcs12 admin 15-13
crypto pkcs12 eap 15-13

D

delete 20-7, 24-7
dhcp 24-8
diag 24-9
dir 20-8, 24-10
disable 2-2

E

enable 2-3

F

fver 24-11

H

help 3-6, 24-12
history 3-7
hit-sample-rate 14-16

I

install soda agent 20-10

L

load config 20-11
ls 24-13

M

md5 20-13
mkdir 20-14
monitor port counters 4-10

N

next 24-14

P

ping 7-20

Q

quit 2-4

R

reset 24-15
reset {ap | dap} 11-12

reset port 4-14
reset system 20-16
rmdir 20-19
rollback security acl 14-8

S

save config 20-20
save trace 21-4
set {ap | dap} bias 11-18
set {ap | dap} blink 11-19, 11-28
set {ap | dap} contact 11-25
set {ap | dap} image 11-29
set {ap | dap} location 11-29
set {ap | dap} name 11-30
set {ap | dap} radio antenna-location 11-31
set {ap | dap} radio antennatype 11-32
set {ap | dap} radio auto-tune max-power 11-33
set {ap | dap} radio auto-tune max-retransmissions 11-34
set {ap | dap} radio channel 11-35
set {ap | dap} radio min-client-rate 11-34, 11-36
set {ap | dap} radio mode 11-38
set {ap | dap} radio radio-profile 11-39
set {ap | dap} radio tx-power 11-40
set {ap | dap} upgrade-firmware 11-44
set accounting {admin | console} 8-22
set accounting {dot1x | mac | web} 8-24
set accounting system 8-26
set arp 7-22
set arp agingtime 7-23
set authentication admin 8-27
set authentication console 8-29
set authentication dot1x 8-31
set authentication mac 8-35
set authentication proxy 8-37
set authentication web 8-38
set auto-config 3-8
set banner motd 3-10
set boot configuration-file 20-21, 20-23
set boot image 20-22
set confirm 3-11
set dap 4-15
set dap auto 11-13
set dap auto mode 11-15
set dap auto persistent 11-16
set dap auto radiotype 11-17
set dap boot-ip 11-20
set dap boot-switch 11-22
set dap boot-vlan 11-24
set dap fingerprint 11-26, 11-149
set dap force-image-download 11-27
set dap security 11-42
set domain security 9-5
set dot1x authcontrol 17-12
set dot1x key-tx 17-14
set dot1x max-req 17-15
set dot1x port-control 17-16
set dot1x quiet-period 17-17
set dot1x reauth 17-18
set dot1x reauth-max 17-19
set dot1x reauth-period 17-20
set dot1x timeout auth-server 17-21
set dot1x timeout supplicant 17-22
set dot1x tx-period 17-23
set dot1x wep-rekey 17-24
set dot1x wep-rekey-period 17-25
set enablepass 2-5
set fdb 5-8
set fdb agingtime 5-9
set igmp 13-3
set igmp lmqi 13-4
set igmp mrouter 13-5
set igmp mrsol 13-6
set igmp mrsol mrsi 13-7
set igmp oqi 13-8
set igmp proxy-report 13-9
set igmp qi 13-10
set igmp qri 13-11
set igmp querier 13-12
set igmp receiver 13-13
set igmp rv 13-14
set interface 7-24
set interface dhcp-client 7-25
set interface dhcp-server 7-26
set interface status 7-28
set ip alias 7-29
set ip dns 7-30
set ip dns domain 7-31
set ip dns server 7-32
set ip https server 7-33
set ip route 7-34
set ip snmp server 7-36
set ip ssh 7-37
set ip ssh server 7-38
set ip telnet 7-39
set ip telnet server 7-40
set length 3-12
set license 3-13
set location policy 8-40
set log 23-3
set log buffer 23-3
set log console 23-3
set log current 23-3
set log mark 23-6
set log server 23-3
set log sessions 23-3
set log trace 23-3
set mac-user 8-43
set mac-user attr 8-44
set mac-usergroup attr 8-50
set mobility profile 8-52
set mobility-domain member 9-6
set mobility-domain mode member seed-ip 9-7
set mobility-domain mode seed domain-name 9-8
set mobility-profile mode 8-54
set network-domain mode member seed-ip 10-6
set network-domain mode seed domain-name 10-8
set network-domain peer 10-7
set ntp 7-41
set ntp server 7-42
set ntp update-interval 7-43
set port 4-17
set port media-type 4-19
set port mirror 4-20
set port name 4-21
set port negotiation 4-22
set port speed 4-24
set port trap 4-25
set port type wired-auth 4-26
set port-group 4-18
set prompt 3-14
set qos cos-to-dscp-map 6-3
set qos dscp-to-cos-map 6-4
set radio-profile active-scan 11-45
set radio-profile auto-tune channel-config 11-46
set radio-profile auto-tune channel-holddown 11-48
set radio-profile auto-tune channel-interval 11-49
set radio-profile auto-tune channel-lockdown 11-50
set radio-profile auto-tune power-backoff-timer 11-51
set radio-profile auto-tune power-config 11-52
set radio-profile auto-tune power-interval 11-53
set radio-profile auto-tune power-lockdown 11-54
set radio-profile auto-tune power-ramp-interval 11-55
set radio-profile beacon-interval 11-56
set radio-profile countermeasures 11-57
set radio-profile dtim-interval 11-58
set radio-profile frag-threshold 11-59
set radio-profile max-rx-lifetime 11-61
set radio-profile max-tx-lifetime 11-62
set radio-profile mode 11-63
set radio-profile preamble-length 11-66
set radio-profile qos-mode 11-67
set radio-profile rfid-mode 11-68
set radio-profile rts-threshold 11-69
set radio-profile service-profile 11-70
set radio-profile wmm 11-76
set radio-profile wmm-powersave 11-77
set radius 16-9

set radius client system-ip 16-11
set radius deadtime 16-9
set radius key 16-9
set radius proxy client 16-12
set radius proxy port 16-13
set radius retransmit 16-9
set radius server 16-14
set radius timeout 16-9
set rfdetect attack-list 19-9
set rfdetect black-list 19-10
set rfdetect ignore 19-11
set rfdetect log 19-12
set rfdetect signature 19-13
set rfdetect ssid-list 19-14
set rfdetect vendor-list 19-15
set security acl 14-9
set security acl ip icmp 14-9
set security acl ip ip 14-9
set security acl ip tcp 14-9
set security acl ip udp 14-9
set security acl map 14-14
set security l2-restrict 5-10
set server group 16-16
set server group load-balance 16-17
set service-profile attr 11-78
set service-profile auth-dot1x 11-80
set service-profile auth-fallthru 11-82
set service-profile auth-psk 11-84
set service-profile beacon 11-85
set service-profile cac-mode 11-86
set service-profile cac-session 11-87
set service-profile cipher-ccmp 11-88
set service-profile cipher-tkip 11-89
set service-profile cipher-wep104 11-90
set service-profile cipher-wep40 11-91
set service-profile cos 11-92
set service-profile dhcp-restrict 11-93
set service-profile idle-client-probing 11-94
set service-profile keep-initial-vlan 11-95
set service-profile long-retry-count 11-96
set service-profile no-broadcast 11-97
set service-profile proxy-arp 11-99
set service-profile psk-phrase 11-100
set service-profile psk-raw 11-101
set service-profile rsn-ie 11-102
set service-profile shared-key-auth 11-103
set service-profile short-retry-count 11-104
set service-profile soda agent-directory 11-105
set service-profile soda enforce-checks 11-106
set service-profile soda failure-page 11-108
set service-profile soda logout-page 11-109
set service-profile soda mode 11-110
set service-profile soda remediation-acl 11-111
set service-profile soda success-page 11-112
set service-profile ssid-name 11-113
set service-profile ssid-type 11-114
set service-profile static-cos 11-115
set service-profile tkip-mc-time 11-116
set service-profile transmit-rates 11-117
set service-profile user-idle-timeout 11-119
set service-profile web-auth-url 11-121
set service-profile web-portal-acl 11-120
set service-profile web-portal-session-timeout 11-123
set service-profile wep active-multicast-index 11-124
set service-profile wep active-unicast-index 11-125
set service-profile wep key-index 11-126
set service-profile wpa-ie 11-127
set snmp community 7-44
set snmp notify target 7-46
set snmp profile 7-51
set snmp protocol 7-56
set snmp security 7-57
set snmp trap 7-58
set snmp trap receiver 7-59
set snmp usm 7-60
set snoop 22-4
set snoop map 22-6
set snoop mode 22-7
set spantree 12-7
set spantree backbonefast 12-8
set spantree fwddelay 12-9
set spantree hello 12-10
set spantree maxage 12-11
set spantree portcost 12-12
set spantree portfast 12-14
set spantree portpri 12-15
set spantree portvlancost 12-16
set spantree portvlanpri 12-17
set spantree priority 12-18
set spantree uplinkfast 12-19
set summertime 7-63
set system contact 3-15
set system countrycode 3-16
set system idle-timeout 3-19
set system ip-address 3-20, 7-65
set system location 3-21
set system name 3-22
set timedate 7-66
set timezone 7-67
set trace authentication 21-5
set trace authentication mac-addr 21-5
set trace authentication port 21-5
set trace authentication user 21-5
set trace authorization 21-6
set trace authorization mac-addr 21-6
set trace authorization port 21-6
set trace authorization user 21-6
set trace dot1x 21-7
set trace dot1x mac-addr 21-7
set trace dot1x port 21-7
set trace dot1x user 21-7
set trace sm 21-8
set trace sm mac-addr 21-8
set trace sm port 21-8
set trace sm user 21-8
set user 8-55
set user attr 8-57
set user group 8-58
set user password 8-55
set usergroup 8-59
set usergroup attr 8-59
set vlan name 5-11
set vlan port 5-12
set vlan tunnel-affinity 5-13
set web-aaa 8-61
show 24-16
show {ap | dap} config 11-128
show {ap | dap} counters 11-132
show {ap | dap} etherstats 11-137
show {ap | dap} group 11-139
show {ap | dap} qos-stats 11-135
show {ap | dap} status 11-140
show aaa 8-62
show accounting statistics 8-65
show arp 7-68
show auto-tune attributes 11-145
show auto-tune neighbors 11-147
show banner motd 3-23
show boot 20-24
show config 20-26
show crypto ca-certificate 15-15
show crypto ca-certificate admin 15-15
show crypto ca-certificate eap 15-15
show crypto certificate 15-17
show crypto certificate admin 15-17
show crypto certificate eap 15-17
show crypto key domain 15-18
show crypto key ssh 15-19
show dap connection 11-151
show dap global 11-153
show dap unconfigured 11-155
show dhcp-client 7-70
show dhcp-server 7-72
show dot1x 17-26
show fdb 5-14
show fdb agingtime 5-16

show fdb count 5-17
show igmp 13-15
show igmp mrouter 13-19
show igmp querier 13-21
show igmp receiver-table 13-23
show igmp statistics 13-25
show interface 7-75
show ip alias 7-77
show ip dns 7-78
show ip https 7-80
show ip route 7-82
show ip telnet 7-84
show licenses 3-25
show load 3-24
show location policy 8-68
show log buffer 23-7
show log config 23-9
show log trace 23-10
show mobility-domain config 9-9
show mobility-domain status 9-10
show mobility-profile 8-69
show network-domain 10-9
show ntp 7-85
show ntp on page 163 7-12
show port counters 4-28
show port media-type 4-30
show port status 4-31
show port-group 4-29
show qos 6-5
show qos default 6-5
show qos dscp-table 6-6
show radio-profile 11-157
show rfdetect attack-list 19-16
show rfdetect black-list 19-17
show rfdetect clients 19-18
show rfdetect countermeasures 19-21
show rfdetect data 19-23
show rfdetect ignore 19-25
show rfdetect mobility-domain 19-26
show rfdetect ssid-list 19-30
show rfdetect vendor-list 19-31
show rfdetect visible 19-32
show roaming station 5-18
show roaming vlan 5-20
show security acl 14-17
show security acl editbuffer 14-17, 14-18
show security acl hits 14-19
show security acl info 14-20
show security acl map 14-22
show security acl resource-usage 14-23
show security l2-restrict 5-21
show service-profile 11-160
show sessions 18-5
show sessions network 18-7
show snmp community 7-89
show snmp configuration 7-87
show snmp counters 7-90
show snmp notify profile 7-91
show snmp notify target 7-92
show snmp status 7-93
show snmp usm 7-94
show snoop 22-8
show snoop info 22-9
show snoop map 22-10
show snoop stats 22-11
show spantree 12-20
show spantree backbonefast 12-23
show spantree blockedports 12-24
show spantree portfast 12-25
show spantree portvlancost 12-27
show spantree statistics 12-28
show spantree uplinkfast 12-33
show summertime 7-95
show system 3-26
show tech-support 3-28
show timedate 7-96
show timezone 7-97
show trace 21-9
show tunnel 5-23
show version 20-28
show vlan config 5-24

T

telnet 7-98
test 24-18
test rflink 19-35
traceroute 7-100

U

uninstall soda agent 20-30

V

version 24-19